SOUNDTRANSIT

Audit Report

Consultant On & Off-Boarding Practices Audit

Report Number: 2020 - 06 | Report Date: October 1, 2020

Executive Summary

Audit Report No.: 2020 - 06 **October 1, 2020**

WE AUDITED the current Consultant On and Off-Boarding Practices at Sound Transit. Our audit focused on agency consultants, contractors, and extranets users' on-boarding and off-boarding practices including access to Agency assets such as network, badges, and office space.

AUDIT OBJECTIVES were to determine whether the agency has effective controls in place to ensure:

- Policies, procedures and processes are clear and provide guidance to stakeholders at the time of onboarding and off-boarding consultants, contractors, and extranet users.
- The agency maintains complete and accurate records for consultants, contractors, and extranet users.
- Consultants, contractors, and extranet users are on-boarded and off-boarded appropriately.

Our audit examined records from January 1, 2017 to April 15, 2020 and processes in place as of April 30, 2020.

Patrick Johnson

Patrick Johnson
Director, Audit Division

WHAT DID WE FIND?

Sound Transit (ST or the "Agency") increasing the capital project footprint (e.g., ST3) has driven the need for an increase in agency staffing in order to accomplish its ambitious goal of bringing more mass transit for a growing region. In order to staff capital projects and make sure operating programs are adequately supported and affordable, ST hires consultants in addition to permanent staff. To ensure agency assets are safeguarded, and non-ST staff adhere to ST policies & procedures, it is critical that the Agency develops effective consultant on and off-boarding practices.

Almost every division and function at the Agency hires consultants and is responsible for onboarding and off-boarding their respective consultants, playing an important role in this "de-centralized" process.

Though the process is de-centralized, certain resources are provided by the Agency to enable consultants hired on behalf of ST to perform their work effectively. Specifically, network access is granted through the Agency's Information Technology (IT) Services Department, access cards are issued by the Public Safety Division within Operations Department, and spaces are assigned and tracked by Administrative Services Division within Executive Department. Consultants' assets (i.e., ST computer) and/or permissions for cloud based sites are determined by team Program Managers, Project Managers, Project Coordinators, etc. and requested through the Agency IT ticketing system, ServiceNow.

At time of our audit, there were roughly 2,400 active non-ST users in Active Directory and over 3,000 non-ST users with active badges in Lenel system. On average, about 700 spaces (offices/desks) were allocated and utilized by consultants for the audit period.

We conclude that the Agency lacks effective consultant onboarding and off-boarding processes.

Agency policies, procedures, and processes do not provide clear guidance to stakeholders at time of onboarding and off-boarding consultants, contractors, and extranet users. The Agency does not have effective controls in place to reasonably assure that the Agency maintains complete & accurate records for consultants, contractors, and extranet users. Controls and processes over consultant off-boarding are ineffective.

Table of Contents

Background

Sound Transit (ST or the "Agency") increasing the capital project footprint (e.g., ST3) has driven the need for an increase in agency staffing in order to accomplish its ambitious goal of bringing more mass transit for a growing region. To ensure capital projects and operating programs are adequately supported and affordable, ST hires consultants[1] in addition to permanent staff. To ensure agency assets are safeguarded, and non-ST staff adhere to ST policies & procedures, it is critical that the Agency develops effective consultant on and off-boarding practices.

These practices are guided by different policies (e.g., Agency Policy 1100 – Information Security Policy, Agency Policy 1101 – Acceptable Use of Technology Policy, Agency Policy 18 – Access Control Policy, Agency Policy 41 – Space Planning, Space Assignment, and Facility Use Policy, Agency Policy 44 – Asset Management Policy, etc.) and procedures (Space Planning Procedures, Access Control Procedures, etc.) at the Agency. Each of these are designed to ensure that the Agency has effective controls and oversight over consultants and contractors.

Almost every division and function at the Agency hires consultants and is responsible for onboarding and off-boarding their respective consultants; playing an important role in this "de-centralized" process. Consistent with the de-centralized approach, consultants may also be referred to as "contractors", "extranet users" or generalized as "non-ST employees/users" depending on nature of services performed (e.g., non-ST employees providing professional services referred as "consultants") and resources provided to perform the contracted services.

Though the process is de-centralized, certain resources are provided by the Agency to enable consultants hired on behalf of ST perform their work effectively. Specifically, network access is granted through the Agency's Information Technology (IT) Services Department[2], access cards are issued by the Public Safety Division within Operations Department[3], and spaces are assigned and tracked by Administrative Services Division within Executive Department[4]. Consultants' assets (i.e., ST computer) and/or permissions for cloud based sites are determined by team Program Managers, Project Managers, Project Coordinators, etc. and requested through the Agency IT ticketing system, ServiceNow[5].

[1] Term "consultant" includes consultants, contractors, extranet users or non-Sound Transit employees excluding interns, temporary employees, guests, etc. in this context.

[2] Per organizational chart dated April 1, 2020

[3] Per organizational chart dated April 1, 2020

[4] Under "Executive" Department effective May 2020. Formerly Operations Projects & Asset Management Division within Operations Department per Org chart dated April 1, 2020.

[5] The Agency implemented ServiceNow, software platform which supports IT Service Management, effective October 15, 2019. Prior to October 2019, the Agency utilized Service Manager for IT Service Management.

Network access information is granted through the Agency's domain system for "Active Directory[6] (AD) managed by IT. The Agency utilizes Lenel[7] to issue and track access cards and manually tracks/forecasts space assignments[8].

The following table summarizes the number of consultants, contractors, and extranet users the agency had for each category and reporting systems reviewed (Active Directory, Lenel/Badge data, and Space Planning records).

Consultants, contractors, and extranet users		
	Active Directory (AD)	**Lenel**
Enabled/Active (non-ST)	2,406 (40%)	3,001 (65%)
Disabled/Inactive (non-ST)	3,633 (60%)	1,623 (35%)
Total (non-ST users)	**6,039**	**4,624**
Total Users	**8,654[9]**	**6,577[10]**
Overall % of total non-ST vs. Total Users	**77%**	**70%**

Consultants and contractors Space Planning[11]				
	2017	**2018**	**2019**	**2020**
Total non-ST users Occupied spaces[12]	**604**	**653**	**761**	**784**
Total[13] Spaces	**2,030**	**2,114**	**2,664**	**2,723**
Non-ST users vs Total Spaces	**30%**	**31%**	**29%**	**28%**

[6] The Agency utilizes Microsoft platform for the agency's "Active Directory".

[7] The Agency implemented Lenel, open-platform security solutions software, effective March 2018.

[8] The Agency utilizes MS Excel in tracking and forecasting space assignments.

[9] Active Directory (AD) data is as of May 4, 2020 containing 8,654 users and removing non-user related accounts (e.g., test, group accounts, etc.), remaining users were 7,826. Out of 7,826, consultants, contractors, and extranet user related accounts made up of 6,039 or 77% of total. AD records are from 1998 to May 4, 2020.

[10] Lenel data was as of April 15, 2020. Lenel consists of users with activate date of 1989 and until April 2020.

[11] Space Planning data was as of April 15, 2020 and only certain locations are tracked (605, 625, 705, 5th & Jackson, Union, OMF, MOW, etc.). Space Planning tracks and updates the schedule on an annual basis and provides the Agency space forecasting for the next five years. If a consultant has been hired and separated from the Agency in the same year, those users are not reflected in the tracking.

[12] Space Planning data includes "consultants" and "Hotel" spaces (excludes temporary, FTEs). Space Planning started tracking conference rooms effective 2019 and those are excluded.

13 Space Planning record total includes open spaces. There were 590, 463, 676, and 701 open spaces in 2017, 2018, 2019, & 2020 respectively.

Audit Objectives

To determine whether the agency has effective controls in place to ensure:

- Policies, procedures and processes are clear and provide guidance to stakeholders at the time of onboarding and off-boarding consultants, contractors, and extranet users
- The agency maintains complete and accurate records for consultants, contractors, and extranet users
- Consultants, contractors, and extranet users are on-boarded and off-boarded appropriately

Scope and Methodology

We conducted this audit in accordance with Generally Accepted Government Auditing Standards (GAGAS) and the International Standards for the Professional Practice of Internal Auditing (IPPF). 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.

We gained an understanding of current Consultant On and Off-Boarding Practices at ST through document reviews, data analysis, personnel interviews, and walkthroughs. We identified risks in the processes and assessed management controls in place to mitigate those risks. Based on our assessment, we determined to focus on agency consultants, contractors, and extranets users' on-boarding and off-boarding practices including access to Agency assets such as network, badges, and office space.

We reviewed consultant, contractor and extranet user records from January 1, 2017 to April 15, 2020 and we examined policies, procedures, and processes as well as current management controls in place as of April 30, 2020. The scope of the audit was limited to processes related to agency consultants, contractors, and extranet users. Processes and controls related to onboarding and off-boarding of other non-Sound Transit employees such as temporary employees, interns, guests, etc. were not included in the scope. Audit did not review assets such as laptops or other Small & Attractive Assets issued to consultants and contractors.

To determine whether the agency has effective controls in place for consultants, contractors, and extranet users' onboarding and off-boarding practices, we performed the following procedures:

1. To determine whether the agency has the effective controls in place to ensure policies, procedures, and processes are clear and provide guidance to stakeholders at time of onboarding and off-boarding, we performed the following procedures:

    a. We reviewed all applicable agency policies, procedures, process level documentation including ones under development, industry best practices (e.g., ISO 27000, 27001, 27002, etc.), compliance requirements (e.g., Washington State Legislature Guidance or Revised Code of Washington (RCW)) to identify definitions, policies, procedures, processes, and guidance for consultant on and off-boarding.

b. We performed process walkthroughs and interviewed 17 groups/teams to identify consultant on and off-boarding processes utilized by different process owners.

c. We reviewed six contracts and one agency plan to determine whether safety, information security, and other pertinent information is provided to consultants when working at ST campus.

2. To determine whether the agency has the effective controls to ensure the Agency maintains complete and accurate records for consultants, contractors and extranet users, we performed the following procedures:

   a. We selected 20 "new" purchases orders (PO) [14] and 125 associated consultants, contractors, and extranet users from invoices [15] and tested whether non-ST users exist in AD, Lenel/Badge, and Space Planning records and whether the records are complete and accurate.

      i. The selection was based on POs that were opened between 2017 and 2020 and associated with "Architecture & Engineering" (A&E), "Public Works – Construction", "Services – Consulting", "Services – Misc.", and "Services – Prevailing Wages" contracts[16].

   b. We selected another 20 "expired/closed" POs and 162 associated consultants, contractors, and extranet users and tested whether non-ST users exist in AD, Lenel/Badge, and Space Planning records and whether the records are complete and accurate.

      i. The selection was based on POs that were closed/expired between 2017 and 2020 and associated with "Architecture & Engineering" (A&E), "Public Works – Construction", "Services – Consulting", "Services – Misc.", "Misc." contracts and contracts [17] with "blank" description.

   c. We analyzed and compared the following records obtained from Agency process owner teams:

      i. We obtained Active Directory (AD) data as of May 4, 2020 from ST

[14] POs were selected from review and analysis of "PO Summary by Type" and "PO Summary" reports as of May 18, 2020 pulled from Agency Reporting Portal.

[15] Invoices were pulled from the Agency SharePoint sites based on availability and function of certain departments (e.g., A&E contract invoices are stored on SharePoint). For those not available, audit reached out to program managers to obtain the detail listing of consultants working on the contract/PO.

[16] Total "Sum of Award" was $3.4 billion for "New" POs for the audit period, awarded to seven (for two descriptions were blank) departments.

[17] Total "Sum of Award Used" was $706 million for "Closed/Expired" POs for the audit period, awarded to eight (for three descriptions were blank) departments.

IT.

ii. We obtained Lenel/Badge Data[18] as of April 15, 2020 from Public Safety.

iii. We obtained Space Planning data (MS Excel) as of April 15, 2020 from ST Operations.

3. To determine whether the agency has the effective controls to ensure consultants, contractors, and extranet users are on-boarded[19] and off-boarded appropriately, we performed the following procedures:

   a. We obtained "Exit User" tickets' reporting from ServiceNow and Service Manager.
      i. ServiceNow consisted of 156 "Exit User" tickets[20] or requests for the audit period (reporting from October 16, 2019 through May 8, 2020).
      ii. Service Manager consisted of 279 "Exit user" tickets (all)[21] or requests for the audit period (December 15, 2017 through December 11, 2019).

   b. We compared 70 "disabled" users (from the previously selected expired/closed PO sample of 162) in Active Directory against the "Exit User" ticketing records obtained above to determine whether "exit tickets" existed in ticketing systems and whether "exit users" were off-boarded timely.

   c. We compared 156[22] (all) "exit user" tickets from ServiceNow[23] against Active Directory to determine whether network accounts were disabled per stated exit date.

   d. We compared 86[24] (all) "exit user" tickets from ServiceNow against Lenel/Badge system to determine whether badge access was appropriately disabled, including notification to property management companies[25] to disable building access for users (52) (tested Q1, 2020 and Q4, 2019).

   e. We compared 20[26] (all) "exit user" tickets from ServiceNow against Space Planning data to determine whether space planning data was accurate and spaces were marked available upon exit.

[18] Access Control also utilizes MS Excel in tracking consultants' disable dates.

[19] Testing of "on-boarding" users comparing against "new user" tickets was not performed as it was not deemed as a high-risk area based on risk assessment.

[20] Total "Exit User" tickets from ServiceNow were for 222 users of which 66 were for FTEs and 156 or 71% were for consultant for the audit period. One user can have multiple "sub tickets" (on average 6) associated with a ticket. Total tickets submitted were 1442 for 242 users.

[21] Audit was not able to determine the consistency of FTEs vs consultants from ServiceManager report as fields were not properly completed to provide such information.

[22] ServiceNow reporting as of 5/6/2020 selected for assignment group "Service Desk"

[23] "Exit User" ticket records in ServiceNow were from October 16, 2019 through May 8, 2020 thus testing was performed based on these dates.

[24] ServiceNow reporting as of 5/6/2020 selected for assignment group "Facilities – Badge Access"

[25] ST campus buildings 605, 625, 705, and 5th & Jackson are managed by companies other than ST and are notified of "exited" employees on a quarterly basis to disable their badges to limit access to these building.

[26] ServiceNow reporting as of 5/6/2020 selected for assignment group "Space Planning"

Conclusion

Policies, procedures, and processes do not provide clear guidance to stakeholders at time of onboarding and off-boarding consultants, contractors, and extranet users. The Agency does not have effective controls in place to reasonably assure that the Agency maintains complete & accurate records for consultants, contractors, and extranet users. Controls and processes over consultant off-boarding are ineffective. **See Finding #1**

Findings and Recommendations

1. The Agency lacks effective consultant onboarding and off-boarding processes

Effective consultant onboarding and off-boarding process allows (not a full listing):

(1) authorized user access to information, systems, and applications and to prevent/limit unauthorized access,
(2) authorized user access to physical facilities and to prevent/limit unauthorized access,
(3) to prevent loss, damage, theft or compromise of assets and interruptions to organization's operations.
(4) safety and security of employees, consultants, contractors, etc.
(5) contractors receiving appropriate awareness, training, and regular updates on Agency policies, procedures, and processes, as relevant to their job function.

Because the Agency's consultant onboarding and off-boarding process is a decentralized process, there is a need for a consistent process across the Agency. Audit noted that the Agency's consultant on & off-boarding processes are inconsistent across the Agency, some controls exist (e.g., record keeping, IT ticketing system, etc.), however, they are not designed well and/or they are not implemented effectively, and there is a lack of information & communication between teams as well as certain fundamental/defining features, as follows:

Policies, procedures, and processes are inconsistent and some non-existent

Policies, procedures, and process level documentation is fundamental to any process, especially for a de-centralized process. Effective processes start with clear definitions, high-level guiding policies, and detailed process level documentation and procedures.

It has been the intent of the Agency to transform and unify core business practices and processes agency wide to enable staff to consistently do their work efficiently and effectively by establishing and implementing a common set of processes, procedures, best practices, and tools[27].

Best practices also suggest for example, an access control policy shall be established, documented, and reviewed based on business and information security requirements. Further, a formal user registration and de-registration process should be implemented to enable assignment of access rights[28]. Though Access Control Policy was established effective September 2002, it has not been revisited since then and has not been updated.

We reviewed the Agency policies, procedures, and process level documentation and noted the following exceptions:

- For 2 or 40% out of 5 policies reviewed, the policies reference Human Resources (HR) department that is no longer associated with consultant on and off-boarding processes.

[27] The Agency Strategic Priority #4 (Agency SharePoint)
[28] ISO/IEC 27001: 2013 (E), Table A-1, page 13

  - Based on interviews with stakeholders involved including Legal division and the Agency's current practices, HR should not be involved with managing consultants due to potential issues with "co-employment" or "joint employment" perception.

- Consultants, contractors[29], extranet[30] users or non-ST employee users' definitions are not clear.
  - The terms of consultants and contractors are utilized interchangeably, however, certain teams define the terms differently. For example, some teams defined "contractors" as employees who are hired to do construction work in the field. Others defined "contractors" as employees who are on-site, present including temporary workers and partner agency employees.
  - There is no agency wide definition of "extranet" users.
    - Due to unclear definitions, extranet users have been assigned badges and some have been assigned space. For example, 101 or 7.7% of 1307 active extranet users are assigned a space per AD.

- Procedures for consultants' onboarding and off-boarding exist for certain teams, however, the procedures and processes are not clear enough to provide guidance and/or fragmented.
  - For example, "Identification Badge and Access Control Procedures" for "Building Access (#1)" and "ID Badges for Consultants and Contractors (#1B)" both dated March 2020, clearly state that "Complete ServiceNow request for your new consultant or contractor with start date and ending date of the contract", however, there is no mention of the steps involved in "off-boarding" consultants.
  - Space Planning procedures dated July 2012 are not designed well for the following reasons:
    1. There is no mention of the procedures for assigning space to consultants and contractors,
    2. Scope and purpose for Space planning tracking are not defined, and
    3. There is no reference to the current system in use for IT ticketing.
- Some teams have created checklists or "desktop" procedures for onboarding and off-boarding consultants; however, there is no agency-wide guidance on the steps involved in hiring and separating with consultants.
    - For example, IT "Add User – Consultant Process" and "How to Process an Exit User Request" documents were reviewed, however, these were instructions for Service Desk on how to process new users and exit users, not instructions for ST employees who hire and/or separate with consultants.

[29] According to PCAM, Section A.4, Definitions, consultant/contractor/vendor/supplier are the person(s), partnership, joint venture, or company or a corporation which enters into a contract with Sound Transit for the performance of work required by the contract.
[30] According to ISACA Glossary of Terms, an extranet is a private network that resides on the Internet and allows a company to securely share business information with customers, suppliers, or other businesses as well as to execute electronic transactions. An extranet user uses the private network to access the company business information.

Overall, the Consultant on and Off-Boarding process appears to have no ownership at the Agency. In the past, there has been attempts made to update processes related to identifying "co-located" consultants however; it has been more than a year since this update with no progress noted.

The agency's ability to onboard and off board consultants becomes increasingly difficult without clear definitions, and clear and accurate guiding documents (e.g., policies, procedures, and process documentation). Program Managers and Project Coordinators become more dependent upon on unstructured institutional knowledge, resulting in inconsistent contractor management practices; leading to gaps in tracking and database records.

Incomplete and/or inaccurate consultants/contractor records

A complete inventory of consultants, contractors, and extranet users is a foundational building block in contractor management process and a prerequisite to effective contractor onboarding and off-boarding. As the Agency's consultant onboarding and off-boarding process is decentralized, completeness & accuracy of information gathered is even more critical. However, audit observed a high degree of incompleteness and/or inaccuracy of data as noted below, due to inconsistent and ineffective processes around consultant onboarding and off-boarding.

- For 19 or 20% of a sample of 96 non-ST users from "New POs", Active Directory is incomplete and/or inaccurate. For some, Active Directory did not reflect accurate space assignment, some should be disabled, or some disabled accounts should be enabled, etc.

- For 31 or 41% of a sample of 75 non-ST users' tested from "New POs", Lenel/Badge data was incomplete and/or inaccurate. For example, Lenel was incomplete as some maintenance workers have badges issued however, they were not tracked by the Agency.

- For 471 or 16% of all (3001) active badges for non-ST employees (ST major partners), the badges should be disabled in Lenel. These included 362 or 62% of 585 Securitas active badges, 45 or 56% of 80 BNSF employee active badges, and 64 or 15% of 431 active King Country Metro (KCM)[31] employee badges should be disabled.

- Further, the Lenel system was implemented effective March 2018, the system is not utilized fully. The Agency tracks "exit" dates manually in a separate MS Excel and inconsistency noted between the two records.
    - On average, 48% of entries are not found between Lenel and Excel.
    - For 1160 or 53% out of 2205 users with disabled badges, the disable dates are in the future (2021 or later) in Lenel.
    - Out of total of total 3,001 non-ST employee active badges, 1,114 or 37% are set to expire in 2099 of which are half are labeled as "consultants" (560).

[31] A separate management letter has been issued to Public Safety.

- For 7 or 19% of a sample of 37 non-ST users' tested, Space Planning data was incomplete and/or inaccurate such as certain non-ST users with spaces were not reflected in Space Planning records.

- Overall, the audit noted that certain consultants and contractors are not tracked at all by the Agency.
    - For 42 or 26% of a sample of 162 non-ST users from closed/expired POs and nine or 7% of a sample of 125 non-ST users from "New" POs, there was no record of users in Active Directory, Space Planning, or Lenel/Badge data.

Whether all consultants, contractors, or extranet users need to be tracked is a question that needs to be determined by the agency; perhaps based on their function, assets (e.g., badges, laptops, etc.) or access needs. For example, for some contractors who are not assigned any assets or do not need any access, they may need to be aware of the Agency policies and procedures (e.g., ST Agency Safety Plan), changes to them as needed, and may need to take certain mandatory trainings as required by the Agency (e.g., InfoSec training mandated by Acceptable Use of Technology Policy[32], compliance requirements based on Records Management Policy[33], etc.).

Given the decentralized processes at the Agency, practices differ from division to division. Most program managers manually track consultants, contractors, extranet users and for some this tracking is non-existent and rely on vendors to provide such listing. Whether it is manual or system generated; however, none of those systems "talk" to each other or it is a fragmented process. Best practices such as ISO 27002[34] suggest maintaining a central record of access rights granted to a user ID to access information systems and services.

Incomplete and inaccurate listing is not conducive of effective and efficient processes when managing contractors. Less than complete information necessitates non-value add processes (inefficient use of resources and time) and ultimately does not allow to monitor and ensure that the information, assets, premises, employees, etc. are safeguarded.

Users are not off-boarded properly

It is the Agency practice to complete ServiceNow request for employees, contractors, and consultants prior to being hired and at time of resignation/separation form the Agency. "New User" and "Exit User" tickets are the "key" communication mechanism to IT, Space Planning, and Access Control teams from project owners and project coordinators regarding consultants' onboarding and off-boarding.

[32] Information Security Policy, effective May 8, 2017, Section 2.3.2 requires "Users must complete periodic information security training". The policy applies to "anyone" who uses or has access to agency technology.
Policy 1100: Information Security Implementation Guidance and Controls (Standards) v1.1, Section 9.2.3.2, "During Employment" also includes "Providing basic information security awareness training to all information system users, and regular updates in agency policies and procedures, as relevant for their job function, at least annually (p.10).

[33] Agency Policy 2000, Managing Public Records, Section 3.1.2, "The agency maintains public information in information systems that ensure their integrity, protection, and accessibility"

[34] Information Technology – Security Techniques – Code of practice for information security controls (ISO/IEC 27002:2017), Section 9: Access Control, 9.2.2 User access provisioning, p.21.

Because the process is de-centralized, the communication is ever so essential. Based on testing procedures performed, we noted high number of exceptions, as follows:

- For 61 or 85% out of 72 disabled users tested, there were issues such as no exit tickets found. More than half (48 or 67%) were disabled by IT or no data existed for certain users (seven from 2017[35]).

- For 26 or 17% of all (156) individual consultant/extranet user "exit tickets' submitted, Active Directory user network account should be disabled.
    - Out of 24 user exit user requests to "disable account" to IT Service Desk and still active, 14 or 56% of users had accessed Active Directory after "exit user" tickets have been submitted on average after 69 days.

- For 14 or 13% of all (105) exit user tickets tested, badges were not disabled in a timely manner or within 10 days[36] of stated exit date.

- For 7 or 13% of all (52) non-ST users with disabled badges which had access to four campus locations, the separations were not reported to property management companies for Q1, 2020 and Q4, 2019 to limit the consultants' access to campus buildings.

- For 13 or 65% of all (20) exit users tested, users were not found in Space Planning tracking even though exit ticket indicated on-campus space.

- Our audit made the following observations in review of Active Directory:
    - On average, there are 626 days between "last logon" date and the network account "disabled" date for all (2684 or 89% of 3001 disabled users) non-ST users that have been disabled in Active Directory indicating users are not disabled in a timely manner.
    - For 298 or 24% of all 2406 active non-ST users, users have not been logged on to network for 90+ days and may need to be disabled.

The gap in communication of "exit" users appears to be related to staff not submitting the tickets through the Agency ticketing system (ServiceNow). In certain situations, IT has been taking corrective measures and disabling accounts that have not been utilized for some time. For example, roughly 250 user accounts were disabled by IT in August 2018 and another 2,500 or so were disabled again in February 2020.

[35] A separate management letter item has been issued to IT

[36] Internal Audit utilized 10 days as reasonable time period to disable users within the "exit" ticket submission. Per review of Agency Identification Badge and Access Control Procedures, 1B: ID Badges for Consultants and Contractors, the procedure states "Badges not returned will be disabled after the third day". The procedure is not specific as to criteria of within how many days badges should be disabled once "exit" ticket is submitted.

This means that about more than one third of all users in Active Directory have been disabled by IT without an “exit” ticket[37]. It is commended that IT is taking some preventative measures to safeguard ST assets and intellectual property, however, the “key” communication mechanism is not being implemented effectively and efficiently and consultants are not offboarded properly. Even when the exit tickets have been submitted, due to the de-centralized or fragmented processes, the Agency records are not reflected accurately and separated consultants’ may still have access to the Agency assets, premises, and/or intellectual property.

[37] IT submits a “one-time” exit ticket at time of “mass” disabling for audit trail purposes.

Recommendations:

We recommend management to:

- Improve Agency consultant, contractor, extranet user or non-ST employees' management processes including onboarding and offboarding. Improve information & communication among stakeholders involved.

  The following specific procedures are suggested for management consideration:

- Define non-ST users who should be tracked and recorded (scope)
  - Define consultants, contractors, extranet users and their associated rights (e.g., extranet user vs badges and/or space)
- Define roles & responsibilities of process owners (e.g., program managers or project coordinators)
- Revisit policies & procedures on a regular basis and update them as needed
- Formalize ad-hoc practices into specific procedures
  - Define & document processes & controls for onboarding and off-boarding non-ST users
  - Define "timeliness" of updating records and disabling users
  - Define and document processes when ST major partners are involved when onboarding and off-boarding consultants
- Educate and train key stakeholders and users (e.g., program managers, program coordinators, ST major partners, etc.)
  - Ensure processes for onboarding and off-boarding consultants are communicated to process owners, program managers, on a frequent basis
- Assess/evaluate the design of certain controls (e.g., Lenel vs manual tracking for disable dates, Lenel vs major partners/agencies, Lenel vs segregation of duties between functions of authorization, recordkeeping, and asset custody, Space Planning records vs scope/purpose) and adjust as necessary
- Improve ST oversight and monitoring of access rights with major suppliers/partners
- Implement controls to ensure consultant data completeness & accuracy, if no centralized system considered.
  - Consider for a centralized contractor management system
- Improve communication between teams to ensure "exit user" tickets are submitted and communicated properly
- Disable users who should not have access to AD and Lenel/Badge data (including property management companies)
  - Update Space Planning records accordingly

Prepared by: Ted Lucas, Chief Procurement & Contracts Officer
Date: 10/01/2020
Audit: Consultant On & Off-Boarding Practices Audit

Management Response:

Management agrees with the audit report finding

Finding 1:

The agency lacks effective consultant on and off-boarding practices.

Management Response / Action Plan:

Management agrees that there is opportunity to improve the consultant on and off-boarding practices. Actions to improve this area are already underway, some having been triggered by unique needs created by the COVID-19 pandemic.

Efforts to-date include:

- Performed initial inventory of active and inactive consultants based on email credentials.
- Created new email assignment practice for consultants and implemented changes allowing for easier identification and targeted communication.
- Created a process for deactivation of building access for inactive and temporarily inactive consultants.
- Created a tracking system for mandatory COVID-19 training completed by co-located consultants with need to work onsite at the Sound Transit campus.
- In 2019, a cross-functional team provided training to project teams on how to submit new user and exit user requests for consultants.

Efforts planned include:

- Create a cross-functional task force to identify process and control improvement areas.
- Investigate use of the agency's Learning Management System to track required information and training completed by ST consultants.

Management appreciates the recommendations contained in the audit report and will use the recommendations as a resource for the cross-functional task force.

Timeline for corrective action:

Management will identify a lead department and cross-functional task force within 30 days. The task force will meet within 60 days, and will review the recommendations contained in the audit report to develop a project plan within 90 days.