Port of Seattle

INTERNAL AUDIT REPORT

INFORMATION TECHNOLOGY AUDIT

Aviation Maintenance and Facilities & Infrastructure Data Centers

January 1, 2017 – November 15, 2018

ISSUE DATE: December 4, 2018

REPORT NO. 2018-16

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Internal Audit (IA) performed an audit of Aviation Maintenance (AV/M) and Facilities and Infrastructure (F&I) Data Centers/IDFs (Intermediate Distribution Frames) during the period January 1, 2017 through November 15, 2018. The audit was performed to evaluate the effectiveness of the IT general controls over the AV/M and F&I controlled data centers and network (ancillary network, communication or servers) closets. These in-scope rooms contain the airport's servers, applications and network infrastructure, which are critical to airport operations. The audit looked at physical security, cleanliness, fire suppression, emergency power and seismic bracing along with other related controls.

This review identified several areas where action will be necessary to mitigate key risks, or where additional process maturity is warranted, as noted below.

1. <u>Physical Access to Facilities</u>

Facilities should be managed and protected using the principle of least privilege/minimum necessary. All rooms in our sample were protected with varying levels of restricted access. Some were well protected, allowing few individuals access, while others allowed access to hundreds of people with no legitimate business need.

2. <u>Physical Facilities Management</u>

Facilities management should be in line with best practices for data centers and communications rooms using business requirements, laws and regulations and health and safety guidelines. In our sample of 31 rooms, 77% of the rooms contained varying levels of flammable material, clutter and dust, and storage of materials not relevant to the purpose of the rooms. Examples include Christmas trees, old equipment, carts, cable rolls, Styrofoam, plastic wrap and documentation binders. Rooms with gas fire suppression lacked warning signage as required by state law.

3. <u>Protection Against Environmental Factors</u>

Facilities should be protected against fire and water damage. In our sample of 31 rooms, 35% of the rooms did not have fire suppression capability and 55% did not have fire extinguishers. Four rooms had Halon fire extinguishers which are ozone-depleting and do not support the Port's value for being a responsible steward of the environment.

These issues are discussed in more detail beginning on page seven of this report.

We believe that the evidence obtained during the audit provides a reasonable basis for our findings and conclusions based on our audit objectives. We extend our appreciation to Port management and the staff of AV/M, F&I and Information Communications & Technology (ICT) for their assistance and cooperation during the audit.

Glenn C Fernandes

Glenn Fernandes, CPA
Director, Internal Audit

Responsible Management Team

Lance Lyttle, Managing Director Aviation
Stuart Mathews, Director, Aviation Maintenance
Wendy Reiter, Director Aviation Security
Jeffrey Brown, Director, Aviation Facility and Capital Program
Rod Covey, Chief of Police
Randy Krause, Fire Chief
Gary Richer, Senior Manager, Aviation Maintenance
Mike Tasker, Senior Manager, Aviation Facilities and Infrastructure

BACKGROUND

The Port of Seattle (Port) is a public enterprise and employs approximately 2,000 employees. The Port owns and operates SeaTac Airport, conference facilities, fishing and recreational boating marinas, industrial properties, and cruise ship terminals. The airport contains critical public infrastructure and relies on complex technologies and information systems to manage its diverse operations and maintain services for tenants, guests, regulatory agencies, and employees.

Prior Internal Audit reports have reviewed data centers managed by the Information and Communication Technology department. This audit focuses on data centers, server rooms and communications rooms managed by Aviation Maintenance (AV/M) and Facilities & Infrastructure (F&I). These in-scope rooms contain the airport's servers, applications and network infrastructure, which are critical to airport operations. The audit looked at physical security, cleanliness, fire suppression, emergency power and seismic bracing along with other related controls.

AUDIT SCOPE AND METHODOLOGY

We conducted this performance audit in accordance with Generally Accepted Government Auditing Standards and the International Standards for the Professional Practice of Internal Auditing. 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 utilized a risk-based approach from the planning phase to the testing phase of our audit. We gathered information through document requests, research, interviews, observations, and analytical procedures. We assessed significant risks and identified controls to mitigate those risks. The scope of this audit included:

- Data centers, server and communications rooms belonging to AV/M and F&I
- Emergency power generation rooms
- Training processes for fire extinguisher handling and gas fire extinguishing systems
- The airport contains hundreds of relevant facilities for this review, so we stratified our sample by data centers, server rooms, equipment rooms, and equipment cabinets, which resulted in a sample population of 31 rooms (plus four interior and exterior network cabinets). We also reviewed supporting infrastructure, such as battery rooms and diesel generator facilities.

The period audited was January 2017 through November 2018 and included the following procedures:

<u>Physical Access to Facilities</u>

- Obtained physical key ownership, and door access and usage reports, then analyzed to determine whether access to the doors in our sample was for only for individuals with a legitimate business need

<u>Physical Facilities Management</u>

- Performed walkthroughs of a sample of relevant data center, server and communications rooms
- Reviewed the rooms for cleanliness, clutter, inappropriate storage of materials and evidence of eating and drinking within the rooms
- Reviewed evidence of training for fire extinguisher use and gas fire suppression system activation response

- Reviewed the rooms to determine whether equipment racks were appropriately secured and seismically braced
- Reviewed the rooms for gas fire suppression warning signage

Protection Against Environmental Factors

- Performed walkthroughs of a sample of relevant data center, server and communications rooms
- Reviewed the rooms for required fire suppression and fire extinguisher installation
- Reviewed the rooms for sub-floor water sensor operation

SCHEDULE OF FINDINGS AND RECOMMENDATIONS

1) RATING: HIGH

Physical Access to Facilities

All rooms in our sample were protected with varying levels of restricted access. Some were well protected, allowing few individuals access, while others allowed access to hundreds of people with no legitimate business need.

All the rooms in our sample were either secured by multi-factor access control, or physical keys. We reviewed the rooms to assure that they were appropriately restricted to individuals with a legitimate business need for access. Our sample included all rooms that we could identify, managed by AV/M & F&I, which contained servers. Additionally, we included a variety of telecommunications rooms, both large and small. Our observations were as follows:

1) A data center/telecommunication room security policy/standard does not exist. There are no formally defined requirements for who is allowed to have access to the in-scope rooms.
2) There is a procedure requiring visitor sign-in and escorting for the MER-ES, PRCS, CER, FIMS and CUSE rooms, however only the MER-ES and PRCS rooms have sign-in sheets. Additionally, we noted that in two of three visits to MER-ES, we were not asked to sign-in, nor did the escorts sign-in.
3) 58% of the rooms used a physical key and only 19% of the rooms had interior security cameras. Physical key is inherently less secure than multi-factor access control devices, does not log activity, and is more difficult to manage. The Port has recognized the risk of physical key access and the lack of security cameras and has a Capital Improvement Project (CIP #C800935) to add access control and cameras to all telecommunications rooms. However, the CIP has been in existence for 18 months, and is still in the planning phase.
4) Access to MER-ES and PCRS is periodically reviewed and has resulted in reasonable levels of people who have access to these facilities. However, access to MDR-3, the C4 Battery room, (and the various telecommunications rooms) are not periodically reviewed, and has resulted in an excessive number of individuals (1,172 for MDR-3 and 1,645 for the Battery room), most of whom have no legitimate business need for access to the rooms.
5) MDR-3, where 1,172 people have access, has one entry door controlled by a multi-factor access device, and another entry door (unsecured) from a mechanical room, which has physical key access. The C4 Battery room does not have its own access control and is accessed from either the Airport Communication Center, the Emergency Coordination Center or an adjacent electrical room (each of which has multi-factor access devices, which allow 1,447, 1,645 and 1,095 individuals to have access, respectively) This mixing of access types will result in access for people who are not intended to have access.
6) We also note that the security system allows the police and fire departments to have unrestricted access to these rooms. These are highly sensitive rooms allowing access to critical server and network infrastructure and access should be restricted to individuals with a legitimate business need.
7) The excessive access noted in items (5) & (6) above is contrary to the NIST Cybersecurity and HIPAA Security physical security requirements:

   PR.AC-4: Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties.

   § 164.310(a)(2)(ii) – Facility Security Plan – in general physical access controls allow individuals with legitimate business needs to obtain access to the facility and deny access to those without legitimate business need.

Recommendations:

1) Create policy/standard that defines whether a person can have access to data centers, server rooms and telecommunications rooms.
2) Add sign-in sheets to all rooms that are required to have them, and train all individuals who have access to the rooms that visitor and escort sign-in is required.
3) There is a CIP (#C800935) to install multi-factor access control devices and interior security cameras in all telecommunications rooms. Increase the priority of the CIP such that the project is completed within one year.
4) Review the access control for all data centers, server rooms and telecommunications rooms to ensure that only individuals with a legitimate business need are permitted access to the rooms.
5) Modify MDR-3 and the C4 Battery room to not allow access by non-multi-factor access device controlled doors. Ensure that all multi-factor device door access into an individual room uses the same door access list.

Management Response:

Aviation Maintenance respectfully disagrees with the rating of High for this element. Regarding internal controls, Aviation Maintenance believes partial controls are in place, though not adequate to identify non-compliance or misappropriation timely.

That said, in general, we agree with the recommendations provided.

1. Agree. Aviation Maintenance is in the process of drafting a document defining the access needs to the various rooms and will then create a policy/standard. Both of these documents will need to be reviewed and concurrence gained from many other departments including Police, Fire, Security, ICT, InfoSec, F&I, CDD and perhaps others.

2. Agree. Aviation Maintenance will work with ICT, InfoSec and F&I to determine triggers for when sign-in sheets are necessary and identify those locations clearly. AV Maintenance will add sign in sheets to the rooms that require it. Training/discussions will be held annually (or sooner if the need is determined) to review the sheets and requirements.

3. F&I will request project completion within the year. However, with the current construction and time constraints on the necessary employees who will need to be involved, this may not be possible. The project is currently in the notebook stage.

4. Agree. AV/M will review, with ICT, F&I, Police, Fire and Security, all access to the rooms and remove any unnecessary access. These spaces with card access will be added to a regular review cycle. For rooms with physical key access, AV Maintenance will explore re-coring these locations with a more secure key profile. This is considered an interim step until the project noted in recommendation #3 is completed. Aviation division staff strongly support the continued access for Port of Seattle Police and Fire staff to maintain ready access to these spaces to be able to perform effectively in their roles as first responders to all parts of the Airport facility. While some individuals in these groups may be able to be removed, we anticipate the vast majority of frontline responders to remain with access.

5. If possible, F&I will create a work request to have the locks rekeyed for controlled access. These doors will be addressed in the project mentioned above. Note, that due to potential code compliance, changing the operations of these doors may not be possible. Access to the C4 Battery room is through other spaces. Due to what we believe to be code egress requirements,

doors into the C4 Battery room may not able to be secured. This will require more investigation. Access to MDR-3 was not intentionally granted to the large volume of individuals as identified. Rather, as the usage of this space has changed over time, the particular door in question had not been incorporated into an updated appropriate door access group, allowing more individuals than appropriate into this group.

DUE DATE: TBD

2) RATING: MEDIUM

Physical Facilities Management

In our sample of 31 rooms, 77% of the rooms contained varying levels of flammable material, clutter and dust, and storage of materials not relevant to the purpose of the rooms. Examples include Christmas trees, old equipment, carts, cable rolls, Styrofoam, plastic wrap and documentation binders. Rooms with gas fire suppression lacked warning signage as required by state law.

Physical facilities management includes the management of computer facilities, power and communications equipment, in line with laws and regulations, technical and business requirements, vendor specifications, and health and safety guidelines. Our sample included all rooms that we could identify, managed by AV/M & F&I, which contained servers. We additionally included a variety of telecommunications rooms, both large and small. Our observations were as follows:

1) There are job plans for reviewing the in-scope rooms for flammable items, security, proper securing of equipment, emptying trash, etc. However we were unable to identify any policy/standard which formally lays out the requirements for the in-scope rooms, in regards to prohibiting inappropriate storage, flammable items, eating and drinking in the rooms and periodic cleaning.
2) We noted evidence of eating and drinking in 39% of the rooms.
3) We noted appropriate training in fire extinguisher use, but no training for how individuals are to respond when in a room with a gas fire suppression system when it activates.
4) We noted a diesel generator facility with a CO_2 fire suppression system, that was lacking state law and National Fire Protection Association (NFPA) standard #12 required warning signs. We also noted one other room with gas fire suppression (FM200) that was not using appropriate warning signage. We also note that the EPA says the following about CO_2 fire suppression systems:

   "*At the minimum design concentration (34 percent) for its use as a total flooding fire suppressant, carbon dioxide is lethal. At concentrations greater than 17 percent, such as those encountered during carbon dioxide fire suppressant use, loss of controlled and purposeful activity, unconsciousness, convulsions, coma and death occur within 1 minute of initial inhalation of carbon dioxide"*

5) We noted clutter and flammable items in 77% of the rooms. There were two rooms in our sample that had extremely high levels of clutter, debris, discarded equipment, etc.
6) We noted the PRCS (Toll Plaza server room) room is being used as a work bench area. Data centers, server rooms and telecommunications rooms should never be used for purposes other than their primary function, as dust and contaminants should be kept out of the rooms.
7) We noted 26% of the rooms were being used to store materials (Christmas trees, shopping carts, empty buckets, old equipment, plastic bins, etc.) that were not relevant to their primary purpose.
8) We noted that 52% of the rooms had equipment on the racks that was not properly secured, and that 16% of equipment racks (while securely bolted to the floors) lacked seismic bracing.

Recommendations:

1) Create policy/standard that defines the requirements for data center, server room and telecommunications rooms in regards to appropriate storage of materials in the rooms, prohibiting flammable materials and eating and drinking within the rooms, and room cleanliness.
2) Develop training for all individuals who have access to any room with a gas fire suppression system which addresses the dangers of the systems, and the proper action to be taken if the system activates.
3) All rooms that use gas fire suppression should conform to the requirements of WAC 296-24-61703 and NFPA 10 & 12, specifically in regard to the exception noted for signage, but also for the other listed requirements.
4) The diesel power generation room that has the CO_2 fire suppression system should be replaced with a less dangerous form of gas fire suppression system. In the meantime, as noted under bullet point (3) above, adequate signage should be installed outside this room to raise awareness among employees. For example, "*Carbon Dioxide gas can cause injury or death. When alarm operates, vacate immediately*" and "*Carbon Dioxide gas can cause injury or death. When alarm operates, do not enter until ventilated.*"
5) Remove from all telecommunications rooms anything that does not directly support the purpose of the room. Add signage to the rooms to make it clear that the rooms may not be used for storage and that eating and drinking is prohibited.
6) Modify the PRCS room (Toll Plaza) to remove the work benches, or split the room into two separate rooms.
7) Ensure that all equipment on the racks in the telecommunications rooms are properly secured.
8) Ensure that all equipment racks are seismically braced as required by F&I Communications Rooms design standards.

Management Response:

1. Agree. AV Maintenance will work with impacted departments to create a policy/standard that defines the requirements. This will require the adoption and agreement of departments with staff accessing these spaces over which AV Maintenance does not have control.

2. Agree. AV Maintenance is working with Health & Safety and Port Fire to develop a training program. This will be rolled out to affected employees who access those areas.

3. Agree. F&I will review the requirements and make any necessary changes.

4. F&I, in conjunction with Port Fire, will verify the fire suppression system and take necessary measures to evaluate the replacement of this system if it is a CO2 based system. In the meantime, adequate signs will be placed on the door and training will be provided to the people who access the room.

5. Approved signage will be placed in each data center, communications room and telecommunications closet and AV/M will clear out any of their items in the rooms. The majority of the items identified in those rooms are not part of an AV Maintenance sponsored project nor being used by AV Maintenance for storage. AV Maintenance will coordinate with the other departments whose staff accesses these spaces to adhere to the storage requirements.

6. While AV Maintenance agrees with the concept of separating these spaces, there is no available space in the Toll Plaza for AV Maintenance to work in support of the PRCS. Due to the critical nature of this system, and the desire from the customer for rapid response, it is highly important for AV Maintenance staff to be located on site at the toll plaza when work on

the PCRS is being performed, or the system is being monitored. The work that happens in this room is primarily for the parking revenue control system. Aviation Maintenance will continue to work with the Landside Operations employees to attempt to identify space to conduct device repairs. Splitting the room as noted above may cause HVAC performance concerns.

7. Agree. F&I will request ICT and AV/M to review their equipment and ensure it is properly secured.

8. Agree. All racks were installed with seismic restraint, but later additional equipment was installed. F&I will propose a project to address this concern.

DUE DATE: TBD

3) RATING: HIGH

Protection Against Environmental Factors

Facilities should be protected against fire and water damage. In our sample of 31 rooms, 35% of the rooms did not have fire suppression capability and 55% did not have fire extinguishers. Four rooms had Halon fire extinguishers which are ozone-depleting and do not support the Port's value for being a responsible steward of the environment.

Protection against environmental factors includes design and implementation measures such as the installation of specialized equipment and devices to monitor and control the environment. Our sample included all rooms that we could identify, managed by AV/M & F&I, which contained servers. Additionally, we included a variety of telecommunications rooms, both large and small. Our observations were as follows:

1) We noted 11 rooms in our sample with no fire suppression (gas or sprinkler) systems. This includes one large group of rooms (old ACC in the parking structure) which used to have a Halon gas fire suppression system. The Halon tanks are empty, and the room(s) which contain a high level of flammable items, and debris, have no fire suppression system.
2) We noted 17 rooms with no fire extinguishers.
3) We noted four rooms which have Halon fire extinguishers. Halon is a legal gas fire suppressant, which has been banned from production since 1994 after it was determined to deplete the ozone layer in the atmosphere.
4) We note the Central Equipment Room (CER) was built and designed to have a raised sub-floor with water sensors, and that those sensors are no longer operational.

Recommendations:

1) Add fire suppression systems (gas or sprinkler) to all telecommunications rooms.
2) Add fire extinguishers to all telecommunications rooms.
3) Replace all Halon fire extinguishers with non-ozone depleting types.
4) Replace the CER sub-floor water sensors.

Management Response:

1. F&I notes that most of the communications rooms have sprinklers. F&I can create a small project to address any deficiencies found.

2. This item can also be addressed with the above mentioned small project.

3. This issue can also be addressed by the above mentioned small project.

4. F&I will work with Aviation Maintenance to replace the sensors.

DUE DATE: TBD

APPENDIX A: RISK RATINGS

Findings identified during the course of the audit are assigned a risk rating, as outlined in the table below. The risk rating is based on the financial, operational, compliance or reputational impact the issue identified has on the Port. Items deemed "Low Risk" will be considered "Exit Items" and will not be brought to the final report.

Rating	Financial	Internal Controls	Compliance	Public	Port Commission/ Management
HIGH	Large financial impact Remiss in responsibilities of being a custodian of public trust	Missing, or inadequate key internal controls	Noncompliance with applicable Federal, State, and Local Laws, or Port Policies	High probability for external audit issues and/or negative public perception	Important Requires immediate attention
MEDIUM	Moderate financial impact	Partial controls Not adequate to identify noncompliance or misappropriation timely	Inconsistent compliance with Federal, State, and Local Laws, or Port Policies	Potential for external audit issues and/or negative public perception	Relatively important May or may not require immediate attention
LOW/ Exit Items	Low financial impact	Internal controls in place but not consistently efficient or effective Implementing/enhancing controls could prevent future problems	Generally complies with Federal, State and Local Laws or Port Policies, but some minor discrepancies exist	Low probability for external audit issues and/or negative public perception	Lower significance May not require immediate attention
Efficiency Opportunity	An efficiency opportunity is where controls are functioning as intended; however, a modification would make the process more efficient				