Financial Stewardship

Accountability

Transparency

# Port of Seattle Audit Committee

## Internal Audit Update

Glenn Fernandes - Director, Internal Audit

April 7, 2022

Remote Meeting

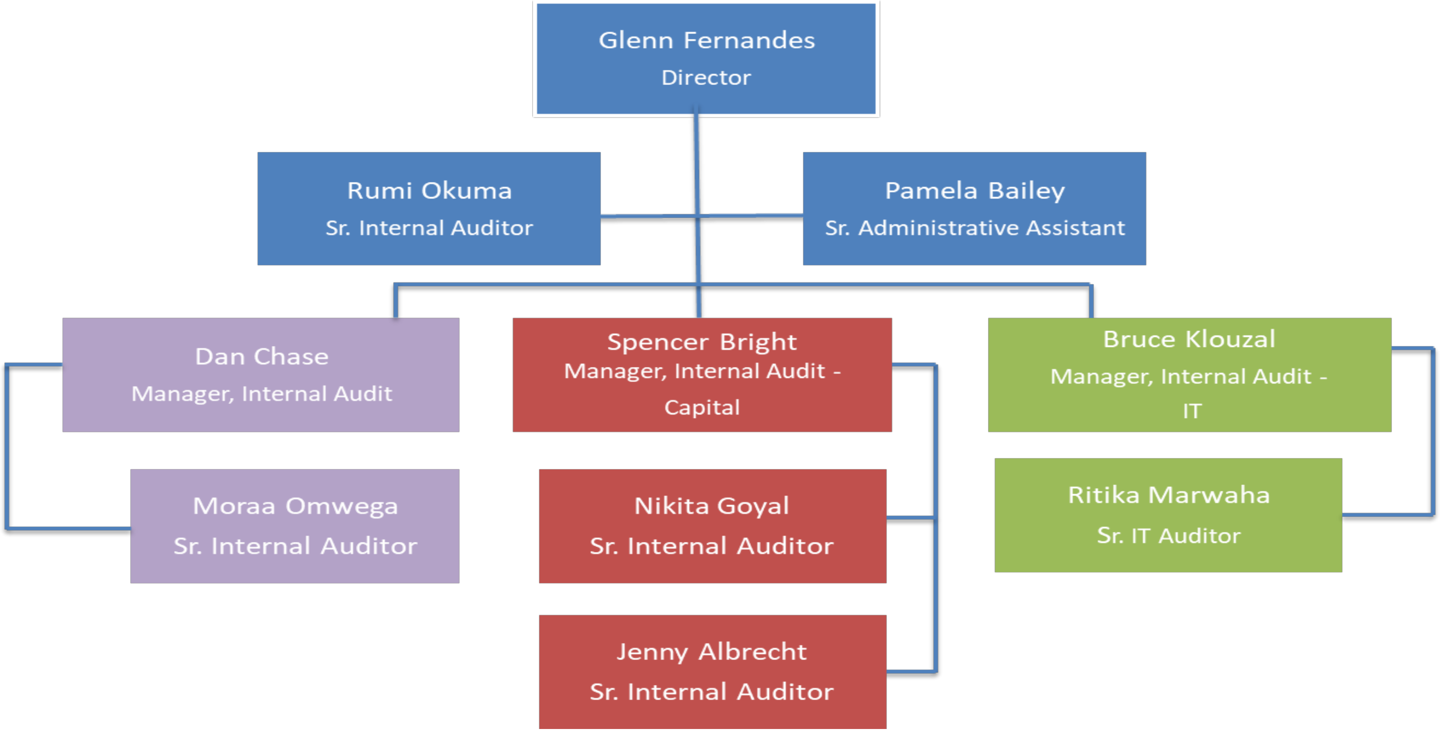
2:30 PM – 4:30 PM

Operational Excellence

Governance

Port of Seattle®

# Internal Audit Organization Structure



Glenn Fernandes
Director

Rumi Okuma
Sr. Internal Auditor

Pamela Bailey
Sr. Administrative Assistant

Dan Chase
Manager, Internal Audit

Moraa Omwega
Sr. Internal Auditor

Spencer Bright
Manager, Internal Audit - Capital

Nikita Goyal
Sr. Internal Auditor

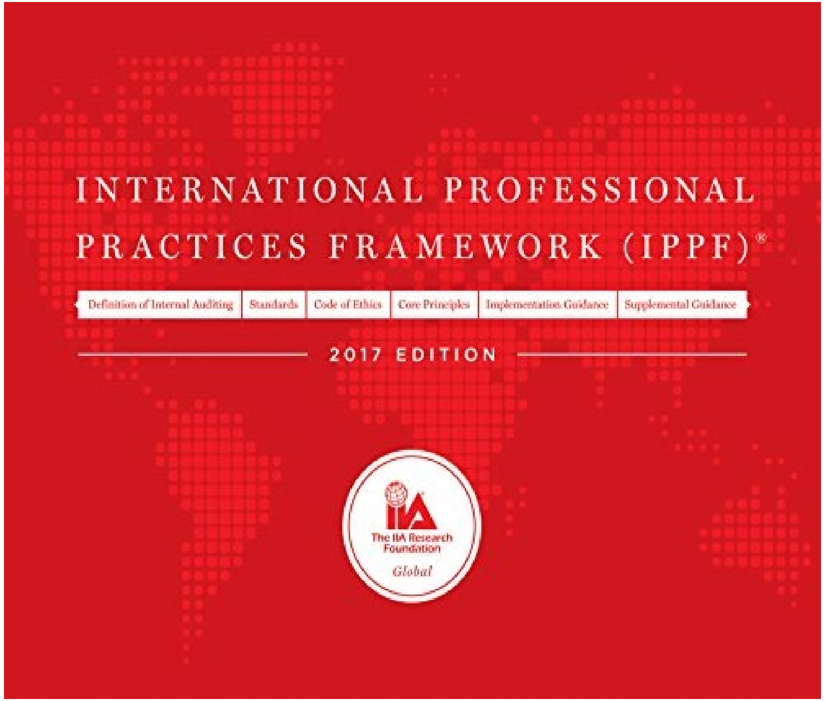
Jenny Albrecht
Sr. Internal Auditor

Bruce Klouzal
Manager, Internal Audit - IT

Ritika Marwaha
Sr. IT Auditor

[Note: In addition, there is one vacant, Senior Internal Auditor position that is deferred to the 2023 budget.]

# Auditing Standards



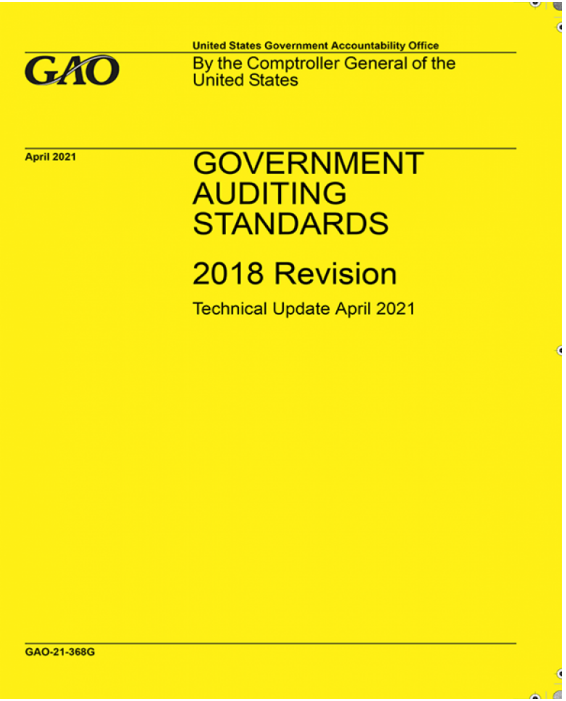
INTERNATIONAL PROFESSIONAL PRACTICES FRAMEWORK (IPPF)®

Definition of Internal Auditing | Standards | Code of Ethics | Core Principles | Implementation Guidance | Supplemental Guidance

2017 EDITION

The IIA Research Foundation

Global



GAO

United States Government Accountability Office

By the Comptroller General of the United States

April 2021

GOVERNMENT AUDITING STANDARDS

2018 Revision

Technical Update April 2021

GAO-21-368G

# Internal Audit Director's Annual Communication

Annual communication required by the Institute of Internal Auditors' International Standards for the Professional Practice of Internal Auditing (IIA Standards) on:

- Organizational Independence
- Internal Audit Charter
- Quality Assurance and Improvement Program
- Open Issue Follow-up and Monitoring Process

# Independence Requirement

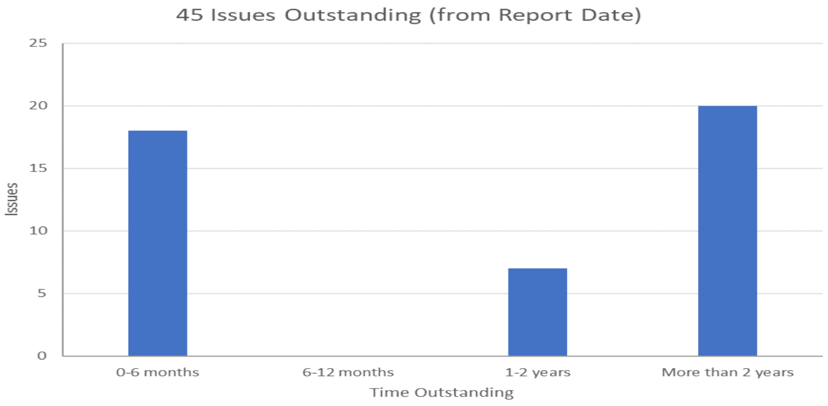
- IIA Standard 1110 requires annual confirmation of organizational independence.

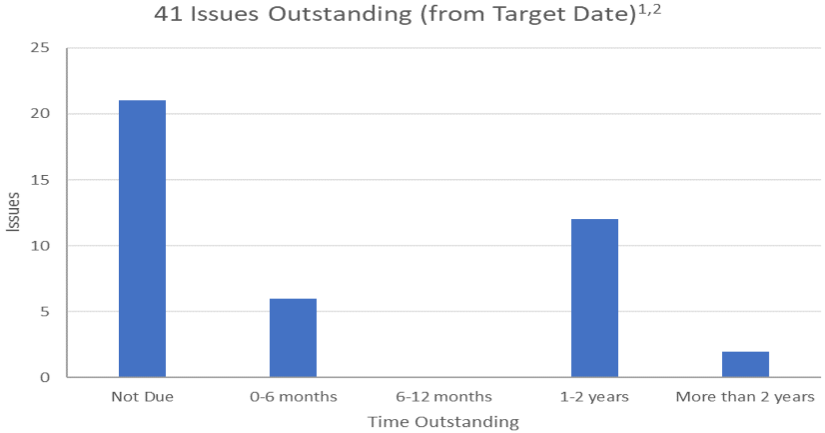
- Internal Audit Department (IA) continues to maintain organizational independence by reporting functionally to the Audit Committee and administratively to the Executive Director.

# Quality Assurance Requirement

- IIA Standard 1310, 1311, and 1312 require both an internal and external quality assurance and improvement program. External assessments (Peer Reviews) need to occur at least every five years.
- Generally Accepted Government Auditing Standards (GAGAS)/Government Accountability Office (GAO) require an external peer review every three years.
- Most recently, in December 2018, an external peer review was conducted by the Association of Local Government Auditors (ALGA).
  - Currently, we are in the process of scheduling the ALGA external peer review for later this year.
- IA's annual self-assessment was last performed in August 2021.
  - Reviewed IA's written polices and procedures (IA Handbook); internal monitoring procedures; a sample of audit engagements and workpapers; and interviewed management and staff on the IA Handbook.
  - Assessment concluded that IA's internal quality control system was suitably designed and operating effectively to provide a reasonable assurance of compliance with GAGAS and IIA Standards. It offered some enhancement opportunities.

# Open Issue Status – Aging Report as of April 7, 2022





1. Fourteen issues outstanding for over one year from the Target Date consist of:

   - **Concourse Concessions LLC (1) - Port RE-2 Policy Review Need/Surety Amount Inconsistency:** SEA intended to perform a complete analysis on the ADR lease requirements, with the participation by core departments (AV Commercial Management, Legal, Finance & Budget, and AFR); however, this effort has been on hold due to priorities such as tenant economic relief programs. A more definitive timeline for completion will be established by management.
   - **Architecture & Engineering (4) - Fair and Reasonable Rate Determination; Management Review Over Max Rates; Contract Rate Accuracy; and Governance**: A lean project to evaluate the rate negotiation process was scheduled for Q1, 2022. Resource constraints has made it challenging to resolve the audit issues. A Governance team has been selected; meetings to begin in 2022.
   - **Information Technology Audits (9) (Security Sensitive) - Exempt from Public Disclosure per RCW 42.56.420 – Issues Not Discussed in Public Session.** They are: Security of Personal Identifiable Information (2), HIPAA Security (4), Closed Network System Security (1), and Network Password Management (2).

2. Four Information Technology issues do not have Target Dates and are not included in this chart. These issues are in the process of being addressed, however, they are more than two years past the Report Date: Disaster Recovery Capability (1), and Aviation Maintenance and Facilities & Infrastructure Data Centers (3).

See **Appendix D** for a detailed listing of outstanding issues aging as of April 7, 2022.

# Approved 2022 Audit Plan

## Limited Contract Compliance

- In-Ter-Space Services, Inc. DBA Clear Channel Airports
- Avis Budget Car Rental
- The Hertz Corporation

## Operational

- Payroll Controls
- Emergency Procurement
- Federal Grant Administration (CRRSA & ARP)
- Community & Sustainability Initiatives

<u>Capital</u>

- International Arrivals Facility (IAF)
- Interim Westside Fire Station
- North Satellite (NSAT) Renovation & Expansion Closeout
- South Satellite (SSAT) High Voltage AC Infrastructure Upgrade
- Post IAF Airline Realignment[2]
- C-1 Building Expansion Construction Phase[2]
- Main Terminal Low Voltage[2]

## Information Technology

- T2 Airport Garage Parking System Replacement[1]
- Account Management (ICT)
- Account Management (Aviation Maintenance)
- Audit Log Management (ICT)
- Audit Log Management (Aviation Maintenance)
- Security Incident Response Management (ICT)
- Security Incident Response Management (Aviation Maintenance)

1. Moved to 2022 audit plan; approved at 6/28/2019 Audit Committee meeting.
2. RCW 39.10.385 requires an independent auditor to perform an audit of subcontractor changes to the Port on GCCM projects, where the subcontractor was selected through an alternative selection process. This audit work will be performed by external, contractor auditors under Internal Audit's supervision, and will be an ongoing, multi-year project through an IDIQ contract.

# 2022 AUDIT PLAN STATUS

| Audit Title | Type | Jan | Feb | Mar | Apr | May | Jun | Jul | Aug | Sep | Oct | Nov | Dec |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| ACH Payment Fraud[1] | Operational | 🟩 | 🟩 | 🟩 | | | | | | | | | |
| Emergency Procurement | Operational | | | | 🟨 | 🟨 | 🟨 | | | | | | |
| Payroll Controls | Operational | | | | | | 🟧 | 🟧 | 🟧 | | | | |
| Federal Grant Administration (CRRSA & ARP) | Operational | | | | | | 🟧 | 🟧 | 🟧 | | | | |
| Community & Sustainability Initiatives | Operational | | | | | | | | | 🟧 | 🟧 | 🟧 | |
| Interim Westside Fire Station | Operational - Capital | 🟩 | 🟩 | 🟩 | | | | | | | | | |
| North Satellite (NSAT) Renovation & Expansion Closeout | Operational - Capital | | | | 🟨 | 🟨 | 🟨 | | | | | | |
| South Satellite (SSAT) High Voltage AC Infrastructure Upgrade | Operational - Capital | | | | 🟨 | 🟨 | 🟨 | | | | | | |
| International Arrivals Facility (IAF) | Operational - Capital | | | | | | | 🟧 | 🟧 | 🟧 | 🟧 | 🟧 | |
| Post IAF Airline Realignment[2] | Operational - Capital | | | | | | | | | | | | |
| C-1 Building Expansion Construction Phase[2] | Operational - Capital | | | | | | | | | | | | |
| Main Terminal Low Voltage[2] | Operational - Capital | | | | | | | | | | | | |
| Account Management (ICT) | IT | 🟩 | 🟩 | 🟩 | | | | | | | | | |
| Account Management (Aviation Maintenance) | IT | 🟩 | 🟩 | 🟩 | | | | | | | | | |
| Audit Log Management (Aviation Maintenance) | IT | | | 🟨 | 🟨 | 🟨 | 🟨 | | | | | | |
| Security Incident Response Management (ICT) | IT | | | 🟨 | 🟨 | 🟨 | 🟨 | 🟨 | | | | | |
| Security Incident Response Management (Aviation Maintenance) | IT | | | | | | | 🟧 | 🟧 | 🟧 | | | |
| T2 Airport Garage Parking System Replacement[3] | IT | | | | | | | 🟧 | 🟧 | 🟧 | 🟧 | 🟧 | |
| Audit Log Management (ICT) | IT | | | | | | | | | | 🟧 | 🟧 | |
| The Hertz Corporation | Contract Compliance | 🟨 | 🟨 | 🟨 | 🟨 | | | | | | | | |
| In-Ter-Space Services, Inc. dba Clear Channel Airports | Contract Compliance | | | 🟨 | 🟨 | 🟨 | | | | | | | |
| Avis Budget Car Rental | Contract Compliance | | | | | | 🟧 | 🟧 | 🟧 | 🟧 | | | |

| | |
|---|---|
| **KEY** | 🟩 Complete |
| | 🟨 In Process |
| | 🟧 Not Started |

1. This audit was added as part of the Port's action to mitigate emerging fraud risk.

2. RCW 39.10.385 requires an independent auditor to perform an audit of subcontractor changes to the Port on GCCM projects, where the subcontractor was selected through an alternative selection process. This audit work will be performed by external, contractor auditors under Internal Audit's supervision, and will be an ongoing, multi-year project through an IDIQ contract.

3. Due to implementation delays, this audit was deferred to the 2022 Audit Plan.

# Audits Completed in the First Quarter, 2022

1) ACH Payment Fraud
2) Interim Westside Fire Station
3) Account Management (ICT)*
4) Account Management (Aviation Maintenance)*

* Security Sensitive – Exempt from Public Disclosure per RCW 42.56.420 – Report Not Discussed in Public Session.

# ACH Payment Fraud

- Internal Audit (IA) completed a targeted audit of the processes that contributed to eight payments totaling $572,682.79, being wired into fraudulent bank accounts.

- The payments were for the Port of Seattle's (Port's) Opportunity Youth Initiative and were intended for the Seattle Parks Foundation (Seattle Parks) and the Urban League of Metropolitan Seattle (Urban League).

- The purpose of the audit was to identify the control breakdowns that allowed the fraud to occur and to recommend ways to reduce the likelihood of future misappropriations.

- The criminal aspect of this case was handed off to the Port Police for their continuing investigation.

# Fraud Overview

Seattle Parks Foundation

- Falisha Kurji – Coordinator
- Email compromised
  - Funds wired to fraudulent accounts

    $184,675.02 ($48,997.39 returned)

Spoofed Domain names copied and used as bait:

Michelle@SeattlePraksFoundation.org

(“Parks” changed to “Praks”)

Michelle Benetua – Director of Strategic Partnerships and Programs

Urban League

- Latonya Stuckey, A/P Specialist
- Email compromised
  - Funds wired to fraudulent accounts

    $388,007.38

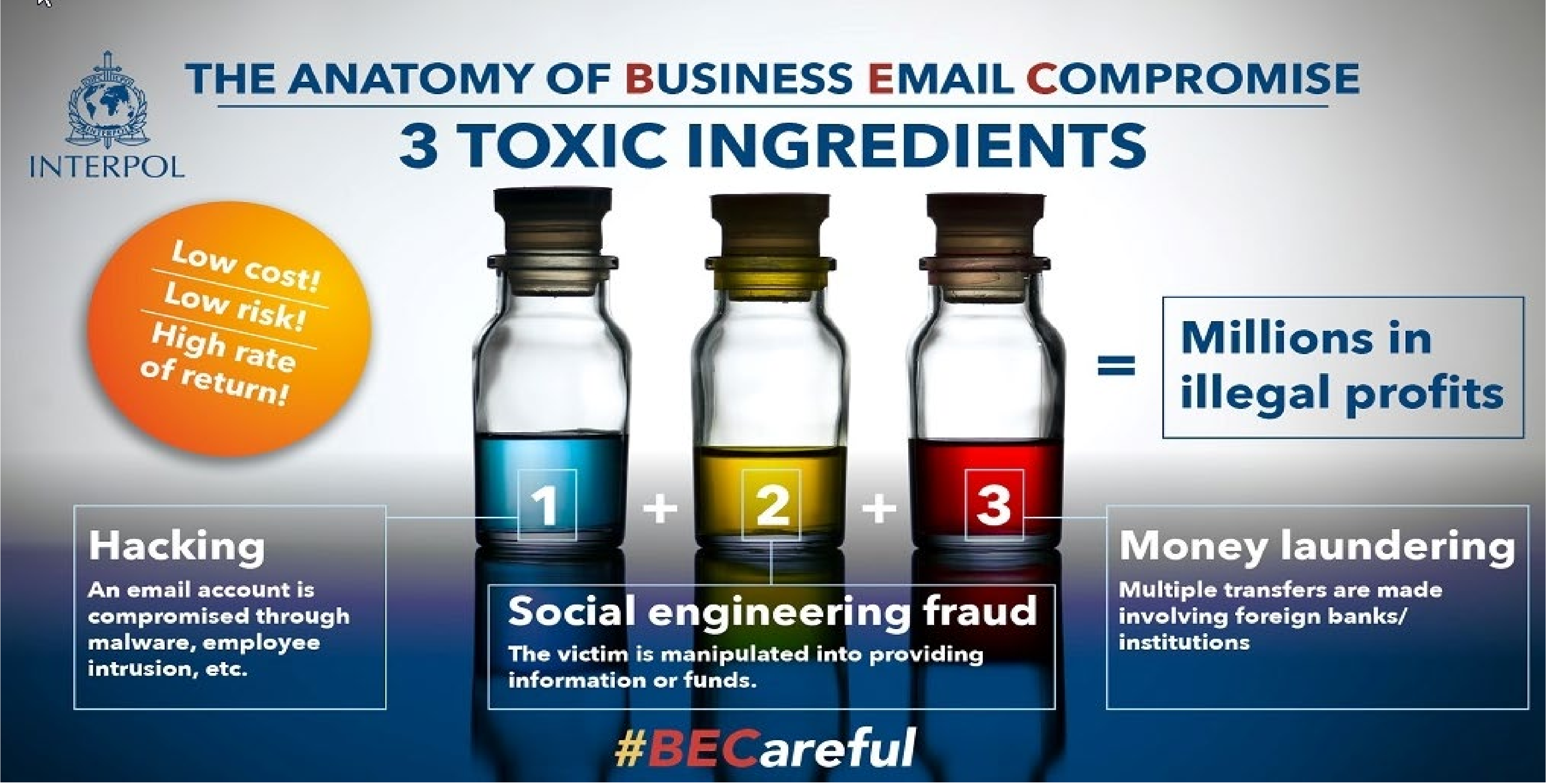
Spoofed Domain names copied and used as bait:

mcamara@urbanIeague.org

jdelapena@urbanIeague.org

alawton@urbanIeague.org

(lower case “l” changed to upper case “I”)



INTERPOL

# THE ANATOMY OF BUSINESS EMAIL COMPROMISE

## 3 TOXIC INGREDIENTS

Low cost!
Low risk!
High rate of return!

1 + 2 + 3 = Millions in illegal profits

### Hacking

An email account is compromised through malware, employee intrusion, etc.

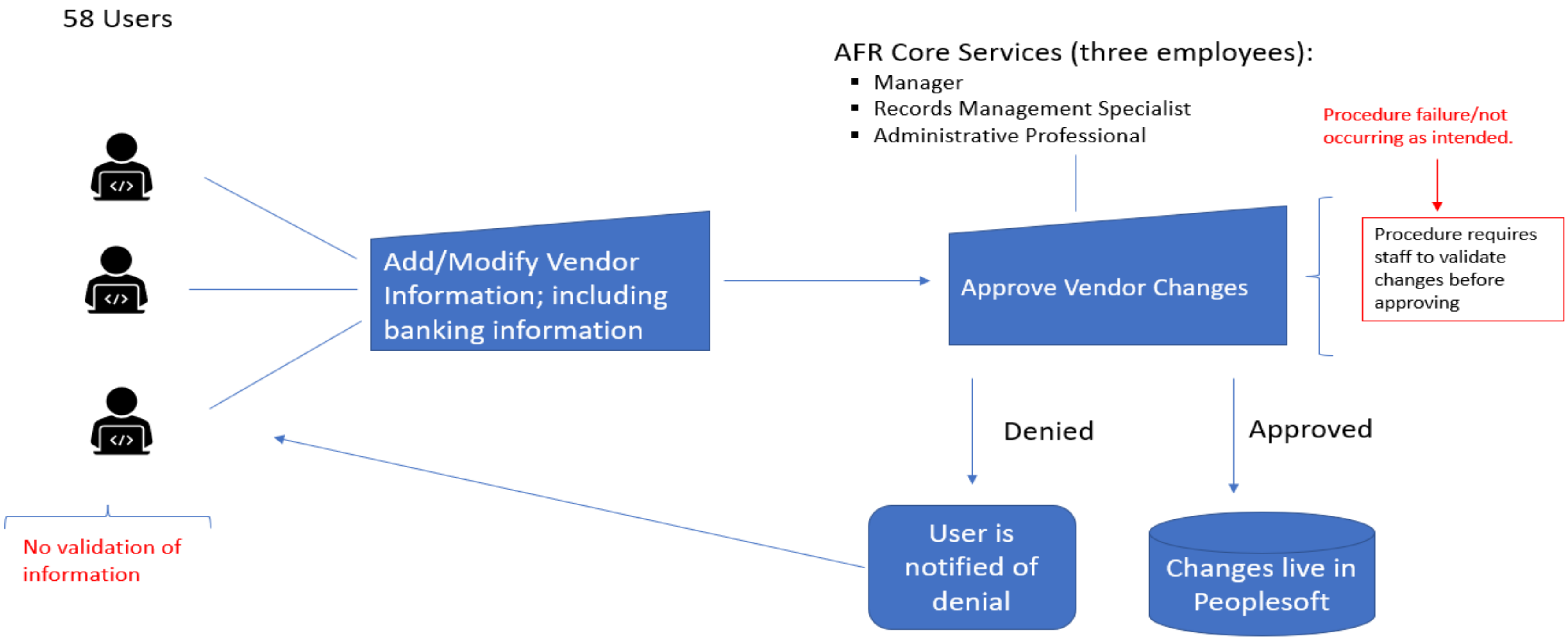
### Social engineering fraud

The victim is manipulated into providing information or funds.

### Money laundering

Multiple transfers are made involving foreign banks/ institutions

#BECareful



58 Users

No validation of information

Add/Modify Vendor Information; including banking information

AFR Core Services (three employees):

- Manager
- Records Management Specialist
- Administrative Professional

Approve Vendor Changes

Procedure failure/not occurring as intended.

Procedure requires staff to validate changes before approving

Denied

Approved

User is notified of denial

Changes live in Peoplesoft

**1) Rating: High**

## Internal controls to validate changes to supplier information, including banking information, were not functioning as intended. Supervisory oversight needed improvement for this critical role.

- The Administrative Professional tasked with approving these changes was not performing the appropriate verification of changes, as required.
- When documented processes are not followed or enforced, internal controls typically do not operate as intended and the likelihood of fraud and errors increase.
- Policy AC-18 needed to be updated to align to current practices.
- The established segregation of duties, are an important control. However, both the individual inputting the data and the individual approving the data, need to do their respective jobs correctly.

# Recommendations

1. We recommend AFR management develop an oversight function to identify, when critical requirements, such as confirming bank account changes, have not been performed. We also suggest that management update any policies that are no longer followed.

2. To aid in authenticating bank information, AFR management should consider investing in a software service that assists in bank verification by providing account holder name, bank name, account holder tax ID number, etc. This vital information will provide the verifier at the Port, the appropriate tools to authenticate changes and additions to bank account information.

**2) Rating: High**

## Procedures to confirm the authenticity of supplier requested bank account changes were not placed at the appropriate level.

- A contributing factor to the fraud was excessive reliance placed on less experienced staff, which allowed them to perform a critical review. The skills required to perform this essential review did not align with the individual’s position within the organization.
- An Administrative Professional had the responsibility to validate and approve supplier requests for all bank accounts changes.
- 1/1/2021 – 1/24/2022 - Port Administrative Professional approved 216 changes and a Record Management Specialist approved 47 changes.
- Additionally, according to Human Resource records, the individual had not attended the Port’s required Information Security Awareness training in both calendar years, 2020 and 2021.

# Recommendations

1. We recommend assigning the approver validation function to an individual with the appropriate skillset, background, and knowledge. This individual should also receive the appropriate training on a regular basis as a requirement of their job.

## 3) Rating: High

**Fifty-eight Port of Seattle employees had the ability to add and modify supplier information, including sensitive banking information, although these changes do not go live in PeopleSoft until the AFR Core Services Team approves them. Adequate controls did not exist to assure that supplier information, including banking and contact information, was entered accurately, consistently, and correctly. Additionally, with the high number of users, the risk of internal fraud increases, because an employee could change bank account data, putting the onus on one individual to approve these changes.**

- A critical piece of information is contact phone number, which is essential, so sensitive information, such as a change to banking account data, can be verified; however, this was not a required field in PeopleSoft.
- Most of the changes did not have phone numbers entered and only a few had email addresses entered.
- A lack of information makes validating the authenticity of the request more difficult.
- Per the AC-18 Supplier Management Policy and Procedures, if a supplier requests a change using email, staff validates the authenticity of the request via a phone call, using the contact information in the supplier module. Conversely, if the request is made via phone call, it is validated through email.

# Recommendations

1. We recommend reducing the number of individuals, who have system access to request additions or modifications to supplier information. We also recommend structuring the supplier module of the PeopleSoft system, so that certain fields are required to be entered (supplier phone number/email address), either via system controls, if possible, or else via policy.

**4) Rating: High**

## Detective controls to identify fraudulent activity and payments did not exist. Instead, the Port was only notified of the fraud by the client, approximately two months after the fact.

- Some detective controls existed within the ACH payment process, including:
  - Senior Disbursements Manager’s daily review of the Accounts Payable journal against payments.
  - Monthly bank reconciliation that agrees payment details.
  - Review of the Wells Fargo report that identifies remittance irregularities, such as the supplier’s bank account cancellation.

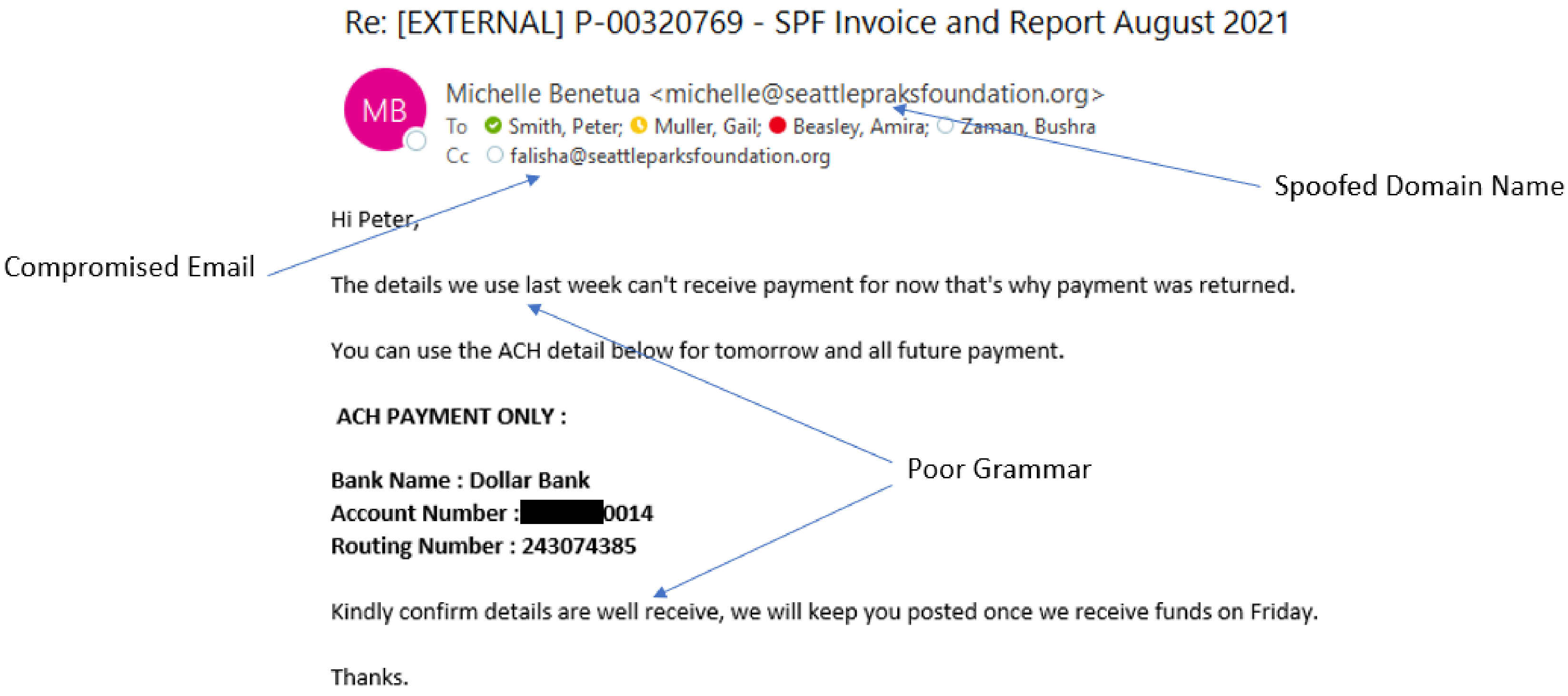
  However, these controls do not necessarily detect fraud.

- If fraud detection controls had existed, management could have identified the breakdown earlier. Instead, both fraud instances were only identified when the suppliers alerted the Port, about 60 days after the initial ACH payments to the fraudsters.

# Recommendations

We recommend implementing general detective controls based on best practices, to detect abnormalities with banking/ACH information changes, these might include:

1. Sending a confirmation notification of any changes to the supplier. This would include banking changes and address changes; if an address changes, it should go to both the old and new addresses.
2. Implementing a management review/sign-off of paperwork/validations for all banking/ACH information changes, utilizing a system generated exception report, to determine if they have met expectations.
3. Monitoring daily ACH payment activity details for abnormalities and timely corrective action, using a fraud focus.



Re: [EXTERNAL] P-00320769 - SPF Invoice and Report August 2021

Michelle Benetua <michelle@seattlepraksfoundation.org>

To ✓ Smith, Peter; ◷ Muller, Gail; ● Beasley, Amira; ○ Zaman, Bushra

Cc ○ falisha@seattleparksfoundation.org

Hi Peter,

The details we use last week can't receive payment for now that's why payment was returned.

You can use the ACH detail below for tomorrow and all future payment.

**ACH PAYMENT ONLY :**

**Bank Name : Dollar Bank**
**Account Number : [redacted]0014**
**Routing Number : 243074385**

Kindly confirm details are well receive, we will keep you posted once we receive funds on Friday.

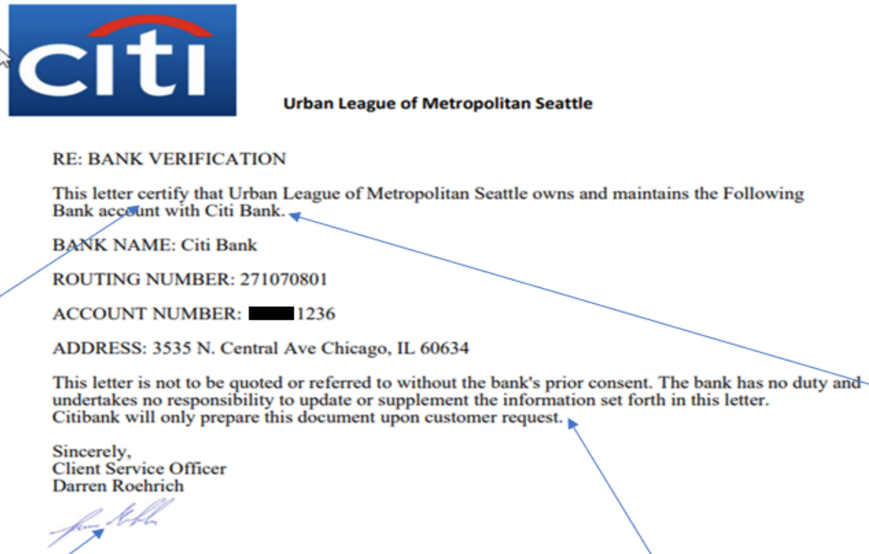
Thanks.

Spoofed Domain Name

Compromised Email

Poor Grammar

Would a bank send you such a letter for a bank account change?



**Urban League of Metropolitan Seattle**

RE: BANK VERIFICATION

This letter certify that Urban League of Metropolitan Seattle owns and maintains the Following Bank account with Citi Bank.

BANK NAME: Citi Bank

ROUTING NUMBER: 271070801

ACCOUNT NUMBER: [redacted]1236

ADDRESS: 3535 N. Central Ave Chicago, IL 60634

This letter is not to be quoted or referred to without the bank's prior consent. The bank has no duty and undertakes no responsibility to update or supplement the information set forth in this letter. Citibank will only prepare this document upon customer request.

Sincerely,
Client Service Officer
Darren Roehrich

Poor grammar

Citibank should be one word (misspelled).

This paragraph would not be typical in a request to change banking information.

Signature does not say Darren Roehrich and is typed below Darren’s name.

**5) Rating: Medium**

## The methodology to assure that vulnerable employees received required training was not functioning effectively. Our review of training records indicated that, of the seven Port employees who either directly or indirectly received the fraudulent emails, only two had completed the Port’s mandatory Information Security Awareness training in 2021. Additionally, Port-wide, only 51 percent or 1,036 of the 2,041 employees had completed the annual training.

- In 2021, the Port required all employees to complete security awareness training (*ICT Information Security Awareness Learning Needs*). Every employee initially received the training upon hire, thereafter employees were required to complete annual refresher training.
- Training topics covered:
  - General Phishing
  - Spear Phishing
  - Business Email Compromise (BEC) Scams
  - Insider Threats

# Recommendations

1. We recommend that all Port employees (and contractors) that are involved in the process of creating, modifying, or requesting changes to supplier banking information, receive additional focused training on cybersecurity and the risks related to Business Email Compromise scams twice per year. If training is not taken, we recommend that user access be disabled until completed.

2. We also recommend that all employees (and contractors) that use a Port computer or have a Port email account, be required to complete the existing Security Awareness Training, and we recommend developing a system to assure that individuals complete such training by the due date.

# Management Response – Issue 1

- Recommendations: We agree.
- Management oversight has been strengthened to ensure that compliance with existing protocols is well documented for all critical validations such as bank account changes. The documentation is stored centrally and reviewed regularly. Extract reports from the Supplier data files are also generated weekly for manager review, including the comments section that documents the validation steps taken for completeness.

**DUE DATE: Completed**

- Policy updates will be made including for any new protocols implemented.

**DUE DATE: In-progress, 5/31/2022**

- A bank account verification service solution is being reviewed with demos already provided by two potential providers. Such a service would augment, not replace, current validation control protocols in place.

**DUE DATE: 4/30/2022 (Vendor selection)**

**Management will discuss in detail. (Full response in Audit Report No. 2022-01)**

# Management Response – Issue 2

- Recommendations: We agree in part.
- We agree that key to any team or individuals performing work effectively is adherence to clearly established policy and procedures, which does exist at the Port, and having the necessary skill sets along with ongoing training. Administrative Professionals at the Port prove themselves to be a very capable and valuable resource. The refinements pursued should not preclude opportunities for and the ability to leverage the talents of Administrative Professionals, by reference to their position or capabilities in the Port organization. Ongoing training and enhanced oversight, as recommended, would support success in this arena.

**DUE DATE: Completed**

**Management will discuss in detail. (Full response in Audit Report No. 2022-01)**

# Management Response – Issue 3

- Recommendations: We agree.
- A controls centric LEAN process improvement project was immediately initiated. This involved the Central Procurement Office and Accounting & Financial Reporting Department, facilitated by the Office of Strategic Initiatives (OSI) certified LEAN specialists. The team identified and is continuing to implement several enhancements, two of which parallel the recommendations.
- Changes have been instituted to the ACH bank account request initiation and verification process. It refines this function to a small, centralized team of about four or five charged with this responsibility. The team includes the manager and lead of the AFR accounts payable operations who make direct contact with the Supplier and then enter and initiate the requests. The requests continue to be administered by the manager and team of the AFR core services operations to independently validate and approve or deny requested additions and changes. The work is performed in conformance with established protocol, is monitored, and will be augmented with ongoing training.

**DUE DATE: Completed**

# Management Response – Issue 3 (continued)

- Changes have been implemented to make the collection of key Supplier information a requirement and at an early point during the procurement process. The objective is that any requests to setup or change Supplier information cannot be initiated unless the required information is obtained and entered to initiate the request process. The substance of this control was implemented earlier on first through procedural controls where requests not containing the required data is denied and returned to the requester. A PeopleSoft Financials system modification that automates the inability to submit and initiate requests if the required Supplier information is not entered in the data fields online, has since been programmed. Testing was completed and this system-driven control has been timely implemented. This action strengthens controls to assure completeness in the Supplier data files for key information.

**DUE DATE: Completed**

**Management will discuss in detail. (Full response in Audit Report No. 2022-01)**

# Management Response – Issue 4

- Recommendations: We agree, with clarification as provided below.
- Although a primary focus continues to be enhancements to strengthen preventative controls, we acknowledge benefits to implementing effective detective controls as well. We look forward to working with Internal Audit to explore any such measures that would offer a reliable protocol to detect fraud. We explored sending a system generated notification triggered by any changes made to the Supplier company. While this is possible to do, this potential detective control relies on Suppliers to be diligent to read their email and, most importantly, reply back to the Port. Bank account pre-noting which auto-generates and sends an email notification to Suppliers is also dependent on replies back to serve as effective detective controls.

**DUE DATE: Under review, 4/30/2022 (Decision)**

- An exception report has been implemented to enhance visibility and management oversight. A central SharePoint library is used to store the documented efforts involving the administration and independent validation of requested additions or changes to Supplier banking information.

**DUE DATE: Completed**

# Management Response – Issue 4 (continued)

- Daily review of bank statement activity, investigating and resolving ACH returns, and pre-review of ACH payments pending release will continue, to assure timely attention for corrective action along with an enhanced fraud focus.

**DUE DATE: Completed**

**Management will discuss in detail. (Full response in Audit Report No. 2022-01)**

# Management Response – Issue 5

- Recommendations: We agree.
- After technical issues with the updated Learning Management System (LMS) tool at the Port of Seattle are resolved through the Human Resources (HR) Department, we expect to see a more accurate listing of individuals who have received annual awareness refresher training. In addition, the Port has recently invested in a more robust cyber awareness training solution through the Information Security Department aimed at user behavior patterns which concentrates training in the areas most needed. The Information Security Department is also currently developing an internal process to monitor and track awareness training based on data from the new training platform.

**DUE DATE: In-progress, 6/30/2022**

- Since this incident, Information Security has conducted advanced training for all teams in the Accounting & Financial Reporting (AFR) Department at their request, which was focused on Business Email Compromises. Similar training is scheduled for all teams in the Central Procurement Office (CPO) including CPO-Purchasing, CPO-Construction, and CPO-Service Agreements.

**DUE DATE: Completed, March 2022 & Ongoing – training throughout the year**

# Management Response – Issue 5 (continued)

- Information Security will continue to offer its monthly cyber awareness seminars, routine messaging, and special learning events to ensure a Port-wide content awareness campaign. This is in addition to the department’s Port intra-net site hosted resources aimed at broadly educating Port staff. Information Security will continue to conduct Phishing exercises, including one recently conducted among 2,244 Port email recipients which has broadened awareness throughout the organization.

**DUE DATE: Ongoing – training throughout the year**

**Management will discuss in detail. (Full response in Audit Report No. 2022-01)**

# Interim Westside Fire Station Project (IWFS)

- The building is a stand-alone, fully functional fire station on the west side of the airfield to meet Federal Aviation Administration (FAA) mandated airfield firefighting requirements.
- This new fire station will provide necessary accommodations to house five firefighters and two Aircraft Rescue Fire Fighting (ARFF) vehicles for 24/7/365 operations.
- Originally approved as a modular building, using the design-bid-build project delivery method with a total project cost of $5.5 million.

| Date | Action | | Amount ($) |
|---|---|---|---:|
| May 2019 | Stand-alone building approval | | 5,500,000 |
| October 2019 | Budget increase | | 3,679,000 |
| February 2021 | Budget increase | | 609,000 |
| September 2021 | Budget increase | | 300,000 |
| | | **Total** | **10,088,000** |

# Interim Westside Fire Station Project (continued)

- In May 2019, the project delivery method was changed to Design-Build as a stand-alone building. Approximately $850,000 was spent prior to the change.
- Macro-Z-Technologies (MZT) was awarded the contract on October 31, 2019, for $4.95 million. With approval of additional days during the Project, Substantial Completion was scheduled to occur on April 23, 2021.
- With approved change orders, the construction contract, with MZT, now stands at $5.6 million.
- Total Project costs to date, including Port soft costs, is $9,010,000.
- The Project is 11 months behind schedule and Substantial Completion has not yet been achieved.

**1) Rating: Medium**

# The Contractor did not complete the Project by the Substantial Completion date, resulting in a delay of use of the fire station.

- On two occasions, the Projects Construction Management (CM) team issued Letters of Forbearance (LOFs). These letters provided MZT an opportunity to meet Substantial Completion without the Port assessing Liquidated Damages (LD). MZT did not respond to either letter.
- On March 4, 2022, the Port issued a letter to MZT and its surety that MZT was in material breach of the contract.
- Estimated liquidated damages to date is $683,000. The Port has withheld $300,000 to cover potential liquidated damages.
- Internal Audit estimates the Port would incur approximately $203,000 in additional inspector costs that were not included in the LD calculation and that it would not be able to assess.

# Recommendations

- Upon completion of the Project, Port management should calculate and pursue liquidated damages from the Contractor.
- Port management should consider contractor performance in future solicitations.

**2) Rating: Medium**

## The Port was potentially overbilled approximately $106,983 out of $140,942 in COVID-19 Not-to-Exceed change orders. Payment for COVID-19 related expenses were approved prior to receiving accurate and complete supporting documentation from the Contractor.

- The intent of this change order was to reimburse MZT for additional costs that would be incurred in order to meet Port's COVID-19 safety requirements beyond  State mandated ones.
- Errors were primarily due to MZT billing when employees were not on-site, and lack of supporting documentation for billed costs.
- The documentation that the Port relies on was not always accurate.
- Opportunity exists for Port management to improve the change order review process, and seek and recover any amount due to the Port.

# Issue 2: COVID-19 Change Order (continued)

| Issue | Questioned Costs ($)<br>Includes 20% Markup |
|---|---|
| The Port was billed for 12 days when a Supervisor was not onsite.<br>One instance where a Supervisor was onsite for six hours but billed eight hours. | $10,467 |
| From September 2020 through February 2021:<br>• One Supervisor was assigned dual duties, not meeting the requirement for a full-time, COVID-19 Supervisor. Internal Audit was not provided documentation to determine the number of daily hours that differentiated between his Supervisory duties and his regular duties.<br>• One Supervisor where Internal Audit was not provided documentation, as requested, to verify the hours billed.<br>• Six instances where the Daily Force Account Field Documents were submitted that included the Supervisor's time, although the Supervisor was not on site.<br>• MZT did not submit Daily Force Account Field Documents for five days. | 87,362 |
| One full-time Supervisor was billed at $89 per hour instead of their actual rate of $52 per hour per change order terms. | 8,568 |
| The Port's Resident Engineer (RE) recommended that MZT be paid $586 without requiring the supporting documentation from MZT. | 586 |
| MZT did not submit Daily COVID-19 written reports of activities, as required. | |
| The Port paid $900 for handwashing stations and disinfection costs even though MZT did not submit receipts, as required. Internal Audit was unable to substantiate the actual costs that MZT incurred. | |
| MZT did not submit actual invoices for subcontractor costs as required by the change order and requested by the Port's RE. The RE created an estimate of costs, however, Internal Audit was unable to substantiate the actual costs of the $20,942 billed to and paid by the Port. | |
| Total Questioned Costs: | $106,983 |

# Recommendations

- Port personnel should require contractors to submit all required supporting documentation related to change orders prior to approving payments. Additionally, given that we have encountered similar results in previous audits where contractors have inaccurately reported labor hours on Daily Force Account Field Documents, we recommend that the Construction Management (CM) Standard Operating Procedures be updated to require contractors submit payroll reports as additional supporting documentation.

- CM should seek and recover any amount due to the Port from the overbilling.

# Management Response – Issue 1

- **Liquidated Damages –** Management agrees that liquidated damages should be imposed for unexcused days. The team fully intends to pursue liquidated damages and that has been previously conveyed to the Contractor.

- **Future Solicitations –** Management agrees and currently has a process to evaluate, including contractor performance in a solicitation. The team intends to review our acquisition planning process to ensure these options are clear for our customers.

**DUE DATE: 12/31/22**

**Management will discuss in detail. (Full response in Audit Report No. 2022-04)**

# Management Response – Issue 2

- **Force Account Requirements –** The Port's Engineering, Central Procurement Office and Legal departments will meet to consider modifications to the Force Account process in future contracts.

- **Recover Any Overbillings –** A reconciliation change order will be issued to close out Change Order 20 based on  validated actual costs incurred by the contractor, once Physical Completion is achieved. We will require the additional documentation identified by Internal Audit from the contractor as part of the validation process and deduct any amounts overpaid.

**DUE DATE: 12/31/22**

**Management will discuss in detail. (Full response in Audit Report No. 2022-04)**

# Appendix

A – Aging of Outstanding Issues as of April 7, 2022

# Appendix A – Aging of Outstanding Issues as of April 7, 2022

## Operational, Capital, Information Technology, and Limited Contract Compliance Audits

| Type | Audit | Description | Rating | Report Date | Target Date | Days Outstanding (from Report Date) | Days Outstanding (from Target Date) |
|---|---|---|---|---|---|---|---|
| IT Audit | AV/M Facility & Infrastructure Data Centers | Security Sensitive | High | 12/4/2018 | No date supplied | 1220 | N/A |
| IT Audit | AV/M Facility & Infrastructure Data Centers | Security Sensitive | High | 12/4/2018 | No date supplied | 1220 | N/A |
| Operational Audit | Marine Maintenance Shop | Keys and badges tracking | High | 6/14/2019 | 12/31/2023 | 1028 | -633 |
| IT Audit | HIPAA Security | Security Sensitive | High | 9/4/2019 | 7/31/2020 | 946 | 615 |
| IT Audit | HIPAA Security | Security Sensitive | High | 9/4/2019 | 7/31/2020 | 946 | 615 |
| Operational Audit | Architecture & Engineering | Determine fair and reasonable | High | 12/9/2019 | 6/30/2020 | 850 | 646 |
| Operational Audit | Architecture & Engineering | Management review over max | High | 12/9/2019 | 6/30/2020 | 850 | 646 |
| Operational Audit | Architecture & Engineering | Contract accuracy | High | 12/9/2019 | 6/30/2020 | 850 | 646 |
| IT Audit | Continuous Vulnerability Management | Security Sensitive | High | 11/29/2021 | 12/31/2022 | 129 | -268 |
| IT Audit | Continuous Vulnerability Management | Security Sensitive | High | 11/29/2021 | 12/31/2022 | 129 | -268 |
| IT Audit | Continuous Vulnerability Management | Security Sensitive | High | 11/29/2021 | 12/31/2022 | 129 | -268 |
| Operational Audit | ACH Payment Fraud | Changes to supplier information | High | 3/30/2022 | 5/31/2022 | 8 | -54 |
| Operational Audit | ACH Payment Fraud | Detective controls | High | 3/30/2022 | 4/30/2022 | 8 | -23 |
| IT Audit | Disaster Recovery Capability | Security Sensitive | Medium | 11/29/2017 | No date supplied | 1590 | N/A |
| IT Audit | AV/M Facility & Infrastructure Data Centers | Security Sensitive | Medium | 12/4/2018 | No date supplied | 1220 | N/A |
| IT Audit | Security of Personal Identifiable Information | Security Sensitive | Medium | 2/26/2019 | 12/31/2019 | 1136 | 828 |
| IT Audit | Security of Personal Identifiable Information | Security Sensitive | Medium | 2/26/2019 | 3/31/2020 | 1136 | 737 |
| IT Audit | HIPAA Security | Security Sensitive | Medium | 9/4/2019 | 7/31/2020 | 946 | 615 |
| IT Audit | HIPAA Security | Security Sensitive | Medium | 9/4/2019 | 7/31/2020 | 946 | 615 |
| IT Audit | Closed Network System Security | Security Sensitive | Medium | 9/5/2019 | 6/30/2020 | 945 | 646 |
| IT Audit | Inventory and Control of Hardware Assets | Security Sensitive | Medium | 11/12/2019 | 6/30/2023 | 877 | -449 |
| Operational Audit | Architecture & Engineering | Governance | Medium | 12/9/2019 | 6/30/2020 | 850 | 646 |
| IT Audit | Network Password Management | Security Sensitive | Medium | 3/20/2020 | 12/31/2021 | 748 | 554 |
| IT Audit | Network Password Management | Security Sensitive | Medium | 3/20/2020 | 9/30/2020 | 748 | 462 |
| IT Audit | Network Password Management | Security Sensitive | Medium | 3/20/2020 | 12/31/2020 | 748 | 97 |
| IT Audit | Secure Configuration for Hardware and Software on Mobile Devices, | Security Sensitive | Medium | 8/21/2020 | 12/31/2021 | 594 | 97 |
| IT Audit | Secure Configuration for Hardware and Software on Mobile Devices, | Security Sensitive | Medium | 8/21/2020 | 12/31/2021 | 594 | 97 |
| Lease and Concession Audit | Concourse Concessions LLC | RE-2 policy review | Medium | 9/10/2020 | 12/31/2020 | 574 | 462 |
| IT Audit | Inventory and Control of Software Assets | Security Sensitive | Medium | 11/24/2020 | 12/31/2021 | 499 | 97 |
| IT Audit | Inventory and Control of Software Assets | Security Sensitive | Medium | 11/24/2020 | 12/31/2021 | 499 | 97 |
| IT Audit | Inventory and Control of Software Assets | Security Sensitive | Medium | 11/24/2020 | 12/31/2021 | 499 | 97 |
| IT Audit | Malware Defenses - Aviation Maintenance | Security Sensitive | Medium | 3/17/2021 | 12/31/2022 | 386 | -268 |
| IT Audit | Continuous Vulnerability Management | Security Sensitive | Medium | 11/29/2021 | 6/30/2022 | 129 | -23 |
| IT Audit | Data Recovery | Security Sensitive | Medium | 11/29/2021 | 4/30/2022 | 129 | -84 |
| IT Audit | Account Management - ICT | Security Sensitive | Medium | 3/15/2022 | 12/31/2022 | 23 | -268 |
| IT Audit | Account Management - ICT | Security Sensitive | Medium | 3/15/2022 | 12/31/2022 | 23 | -268 |
| IT Audit | Account Management - ICT | Security Sensitive | Medium | 3/15/2022 | 6/1/2023 | 23 | -328 |
| IT Audit | Account Management - ICT | Security Sensitive | Medium | 3/15/2022 | 3/1/2023 | 23 | -420 |
| IT Audit | Account Management - Aviation Maintenance | Security Sensitive | Medium | 3/22/2022 | 12/31/2022 | 16 | -268 |
| IT Audit | Account Management - Aviation Maintenance | Security Sensitive | Medium | 3/22/2022 | 12/31/2022 | 16 | -268 |
| IT Audit | Account Management - Aviation Maintenance | Security Sensitive | Medium | 3/22/2022 | 12/31/2022 | 16 | -268 |
| Capital | Interim Westside Fire Station Project | Liquidated Damages | Medium | 3/25/2022 | 12/31/2022 | 13 | -268 |
| Capital | Interim Westside Fire Station Project | COVID-19 Change Orders | Medium | 3/25/2022 | 12/31/2022 | 13 | -268 |
| Operational Audit | ACH Payment Fraud | Required training | Medium | 3/30/2022 | 6/30/2022 | 8 | -84 |
| IT Audit | Continuous Vulnerability Management | Security Sensitive | Low | 11/29/2021 | 12/31/2022 | 129 | -268 |