

# INTERNAL AUDIT REPORT



Information Technology Audit  
Security Incident Response Management (ICT and Aviation  
Maintenance)

January 2021 – July 2022

Issue Date: August 11, 2022  
Report No. 2022-09

## TABLE OF CONTENTS

Executive Summary.....	3
Background .....	4
Audit Scope and Methodology.....	6
Appendix A: Risk Ratings.....	7
Appendix B: Center for Internet Security (CIS) Controls .....	8

## Executive Summary

Internal Audit completed an Information Technology audit of the security incident response management processes for the period January 2021 through July 2022. This audit was performed to evaluate the adequacy of internal controls related to the processes for developing and maintaining an incident response capability to prepare, detect, and quickly respond to an attack. The scope of this audit covered the Enterprise network; managed by the Port of Seattle's (Port's) Information and Communication Technology (ICT) department, and the Access Control System (ACS) network, Industrial Control System (ICS) network, and OpsLan network; managed by the Port's Aviation Maintenance (AV/M) department.

Security Incident Response is part of the 18 critical Center for Internet Security (CIS) controls<sup>1</sup>. The CIS security controls are a prioritized set of best practices created to protect organizations and data from cyber-attack vectors. By adopting these controls, organizations can quickly detect the majority of cyber-attacks. A comprehensive cybersecurity program includes protections, detections, response, and recovery capabilities. The primary goal of incident response is to identify threats on the enterprise, respond to them before they can spread, and remediate them before they can cause harm<sup>2</sup>.

Computer security incident response has become an important component of Information Technology (IT) programs. Cybersecurity-related attacks have become not only more numerous and diverse, but also more damaging and destructive. An incident response capability is therefore necessary for rapidly detecting incidents, minimizing loss and destruction, mitigating the weaknesses that were exploited, and restoring IT services.

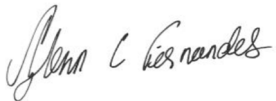
Incident response capability supports responding to incidents systematically so that the appropriate actions are taken. Additionally, information gained during incident handling can be used to better prepare for handling future incidents and to provide stronger protection for systems and data.

Our audit focused on the overall design and effectiveness of the security incident process to assure the protection of critical information and systems.

**Based on the results of our audit, we concluded that the security incident response processes for the Enterprise network and the OpsLan, ACS, and ICS networks, are operating effectively.**

During the course of our audit, Internal Audit identified some opportunities for improvement in the security incident response management processes which were immediately addressed by management upon being notified.

We would like to thank management and staff of Information and Communication Technology, Information Security, and Aviation Maintenance, for their cooperation and responsiveness to our requests during the audit.



Glenn Fernandes, CPA  
Director, Internal Audit

### Responsible Management Team

Matt Breed, Chief Information Officer  
Ron Jimerson, Chief Information Security Officer  
Mike Tasker, Director, Aviation Maintenance

---

<sup>1</sup> See Appendix B – Center for Internet Security (CIS) Controls.

<sup>2</sup> See <https://learn.cisecurity.org/cis-controls-download>

## Background

The Port of Seattle (Port) is a municipal corporation of the State of Washington, organized on September 5, 1911, under the State statute RCW 53.04.010. The Port is composed of three operating divisions, namely, Aviation, Maritime, and Economic Development, and employs approximately 2,000 employees. The Port owns and operates assets, including Seattle-Tacoma International Airport (SEA), conference facilities, fishing and recreational boating marinas, industrial properties, and cruise ship terminals. This Information Technology audit included the following departments in its scope:

*Information and Communication Technology* (ICT) delivers and supports a wide variety of technology solutions to enable Port objectives.

The *Information Security Department* is integrated with ICT, Maritime, and Aviation Maintenance. The department provides strategies, operations, and controls for protecting the Port's information systems and sensitive data, while increasing business resiliency.

*Aviation Maintenance* (AV/M) provides services to support the operations of SEA, its tenants, and guests. Within AV/M, in the Aviation Electrical & Electronic Systems team, the 44 Electronic Technicians (ETs) provide support and maintenance of custom and off-the-shelf operational applications to the airport's business units.

According to the Center for Internet Security (CIS) controls, a comprehensive cybersecurity program includes protections, detections, response, and recovery capabilities. The primary goal of incident response is to identify threats on the enterprise, respond to them before they can spread, and remediate them before they can cause harm. When an incident occurs, if an enterprise does not have a documented plan; it is almost impossible to know the right investigative procedures, reporting, data collection, management responsibility, legal protocols, and communications strategy that will allow the enterprise to successfully understand, manage, and recover.

As per the National Institute of Standards and Technology (NIST) Computer Security Incident Handling Guide<sup>3</sup>, an event is "any observable occurrence in a system or network", while a computer security incident is "a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices".

The incident response lifecycle (Figure 1), consists of four phases:

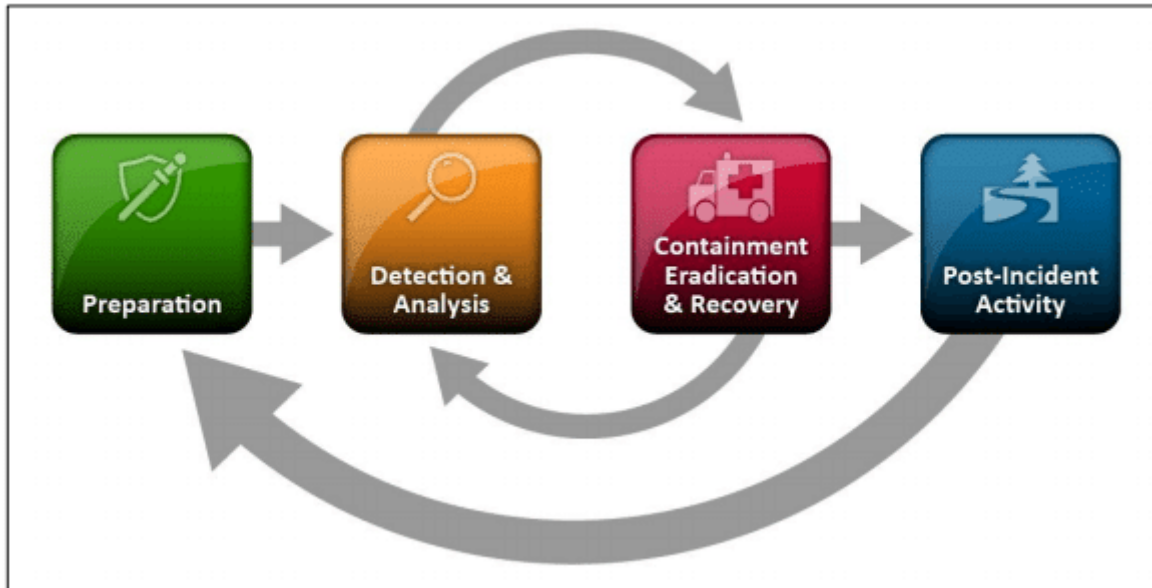
- **Preparation:** Establishing an incident response capability so the organization is ready to respond to incidents, but also preventing incidents by ensuring that systems, networks, and applications, are sufficiently secure.
- **Detection and Analysis:** Determining whether an incident has occurred and, if so, the type, extent, and magnitude of the problem.
- **Containment, Eradication, and Recovery:**
  - a. Containment - provides time for developing a tailored remediation strategy. An essential part of containment is decision-making (e.g., shut down a system, disconnect it from a network, or disable certain functions).
  - b. Eradication - may be necessary to eliminate components of the incident, such as deleting malware and disabling breached user accounts.
  - c. Recovery - restore systems to normal operation, confirm that the systems are functioning normally, and (if applicable) remediate vulnerabilities to prevent similar incidents. Recovery may involve such actions as restoring systems from clean backups, and rebuilding systems from scratch.

---

<sup>3</sup> <https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf>

- **Post-Incident Activity:** Learning from the incident by reviewing what happened and how staff and management performed in dealing with the incident. Lessons learned meetings improve future responses; a post-mortem analysis of the way an incident was handled can expose missing steps or inaccuracies in procedures. The reports gathered from these meetings provide a reference when handling similar events in the future.

*Figure 1 – Source: NIST800-61 Rev 2 Computer Security Incident Handling Guide*



The CIS controls for Incident Response Management, apply to the Port in the following manner:

- 1) **Designate Personnel to Manage Incident Handling**—one official has been designated as the key resource to manage incident handling, and one as their backup, under both the Enterprise and AV/M environments.
- 2) **Establish and Maintain Contact Information for Reporting Security Incidents**—a RACI (Responsible, Accountable, Consulted, and Informed) Chart has been developed to maintain the contact information for reporting security incidents.
- 3) **Establish and Maintain an Enterprise Process for Reporting Incidents**—FreshService, a ticketing system, is utilized to report, manage, and document security incidents for both ICT and AV/M environments. AV/M initially tracks their incidents on Maximo (Asset Management Software) but also informs InfoSec who then also tracks those incidents on FreshService.
- 4) **Establish and Maintain an Incident Response Process**—the Port's Information Security department is responsible for managing incident response activities, including incorporating other Port staff as necessary, based on the nature of the incident.
- 5) **Assign Key Roles and Responsibilities**—key roles and responsibilities have been assigned as documented in the Port's Cyber Incident Response Standard Operating Procedures (SOP).
- 6) **Define Mechanisms for Communicating During Incident Response**—mechanisms used for communicating have been documented in the Cyber Incident Response SOP.
- 7) **Conduct Routine Incident Response Exercises**—routine tabletop exercises are performed by InfoSec and ICT, with top executives and key leadership stakeholders. AV/M also participates in these exercises.
- 8) **Conduct Post-Incident Reviews**—lessons learned, and post incident reviews are performed for major incidents to help improve the response effort.

## **Audit Scope and Methodology**

Internal Audit conducted this Information Technology audit in accordance with Generally Accepted Government Auditing Standards (GAGAS) 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 the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

To achieve the audit objective, Internal Audit used a detailed audit program based on the Center for Internet Security controls. Internal Audit used judgmental sampling methods to determine the samples selected for our audit test work. The results of this work cannot be projected to the population as a whole.

Multiple methodologies were applied to gather and analyze information pertinent to the objective and scope of this audit. The period audited was January 2021 through July 2022. The audit covered polices, processes, and mechanisms in place at the time of the audit. The audit included a review of security incident response processes for the Port's Enterprise network, Access Control System (ACS), Industrial Control System (ICS), and OpsLan networks, and included the following procedures:

### **Policies and Procedures Review**

- Reviewed and assessed policies and procedures related to security incident response management.
- Interviewed personnel to assure knowledge of, and compliance with policies and procedures.
- Reviewed the Cyber Incident Response SOP to verify that roles/responsibilities were defined and aligned with the incident management roles on identifying and determining if an incident had occurred.
- Assessed whether the design of the policies and processes were adequate to address the prevention and detection of cybersecurity threats and reduce the risk of service disruption, and data loss.

### **Process Walkthroughs**

- Performed walkthroughs of security incident response management processes with the following personnel to gain an understanding of the processes and related internal controls:
  - Manager, Information Security
  - Director, ICT Infrastructure Services
  - Electronic Technician (ET) Foreman, Aviation Maintenance

### **Testing**

- Performed testing and review of evidence to determine whether annual reviews were performed for existing processes.
- Performed a review of evidence collected to determine the design and operating effectiveness of the controls being tested, including examples of FreshService tickets and a judgmental sample selection of the Incident Response Timeline Tracking (IRTT) document for Security Incidents, RACI Chart, ICT Priority Response Chart, tabletop exercise presentation materials, etc.
- Reviewed examples of communication that occurred between the responsible officials, upon being notified of an Incident.

## Appendix A: Risk Ratings

Findings identified during the audit are assigned a risk rating, as outlined in the table below. Only one of the criteria needs to be met for a finding to be rated High, Medium, or Low. Findings rated Low will be evaluated and may or may not be reflected in the final report.

Rating	Financial Stewardship	Internal Controls	Compliance	Public	Commission/ Management
<b>High</b>	Significant	Missing or not followed	Non-compliance with Laws, Port Policies, Contracts	High probability for external audit issues and / or negative public perception	Requires immediate attention
<b>Medium</b>	Moderate	Partial controls Not functioning effectively	Partial compliance with Laws, Port Policies, Contracts	Moderate probability for external audit issues and / or negative public perception	Requires attention
<b>Low</b>	Minimal	Functioning as intended but could be enhanced	Mostly complies with Laws, Port Policies, Contracts	Low probability for external audit issues and/or negative public perception	Does not require immediate attention

## Appendix B: Center for Internet Security (CIS) Controls

The Center for Internet Security (CIS) Controls are a recommended set of actions for cyber defense that provide specific and actionable ways to block or mitigate known attacks. Below is a list of the 18 CIS Controls, Version 8.0 which was launched by CIS on May 18<sup>th</sup>, 2021:

1. Inventory & Control of Enterprise Assets	7. Continuous Vulnerability Management	13. Network Monitoring & Defense
2. Inventory & Control of Software Assets	8. Audit Log Management	14. Security Awareness & Skills Training
3. Data Protection	9. Email & Web Browser Protections	15. Service Provider Management
4. Secure Configuration of Enterprise Assets	10. Malware Defenses	16. Application Software Security
5. Account Management	11. Data Recovery	17. Incident Response Management
6. Access Control Management	12. Network Infrastructure Management	18. Penetration Testing