# Data Center Audit

Port of Seattle®

April 2015

*Powerful Insights.*
*Proven Delivery.®*

protiviti®
Risk & Business Consulting.
Internal Audit.

# Table of Contents

This report provides management with information about the condition of risks and internal controls at one point in time.  Future changes in environmental factors and actions by personnel may significantly and adversely impact these risks and controls in ways this report did not and cannot anticipate.

# Executive Summary

## Introduction

In early 2015, Protiviti was engaged by the Port of Seattle ("the Port") to conduct an audit of the data centers and related IT processes supporting operations at Seattle-Tacoma Airport and Pier 69. Fieldwork was conducted between January and February, concluding on February 20, 2015.

## Objective

- Provide an independent assessment of the Port's data center operations and guidance for reducing risk related to the data centers and support practices.
- Determine if adequate infrastructure, processes and related controls are in place to mitigate physical, logical, and environmental risks within the data centers.
- Understand the adequacy of the data centers' ability to perform as recovery sites in the event of a disaster.

# Executive Summary (continued)

## Procedures Performed

The specific scope performed by Protiviti includes the following actions:

- Understand data center architecture and configuration
  - Gather and review existing documentation related to: data center architecture and configurations, applicable data center processes, IT assets within the datacenter, contracts, planning, controls, and key stakeholders.
- Understand and evaluate data center environment
  - Hold interviews with both Aviation Maintenance (AV) and Information Communication and Technology (ICT) personnel to understand data center management processes in more detail.
  - Perform walkthroughs and inspections of in-scope data center locations. Areas of coverage include data center operations, power, environmental, physical security, logical security, monitoring, asset management, and evaluation of BCP/DR capability by location.
- Audit processes and controls
  - Select a sample of devices within the data center and inspect each for adherence to existing policies and industry best practices, power configurations standards, monitoring standards, and asset management standards.
- Report results and observations
  - Develop a report that includes an executive summary of audit results, observations, and recommendations for improvement.

# Executive Summary (continued)

## Areas of Focus and Procedures Performed

- **Power Infrastructure:** Clean, uninterruptable power is essential to ensure the ongoing operations of data centers. Industry best-practices mandate that data centers maintain redundant power feeds, uninterruptable power supplies (UPS), and backup generators. *The Protiviti team conducted a walkthrough of the power sourcing environment, UPS, and generators. A review was conducted of the Preventative Maintenance Inspection (PMI) documentation, monitoring and alerting infrastructure, and overall system design.*

- **Environmental:** Data centers and other areas that house critical systems and infrastructure are designed to operate in certain temperature/humidity ranges. *Protiviti conducted a walkthrough of the Port's data centers and other rooms that house production equipment and infrastructure. The team reviewed environmental monitoring and alerting capabilities and evaluated PMI procedures and documentation.*

- **Physical Security:** Ensures that access to data centers and critical equipment areas are limited to authorized individuals. This access is generally enforced by badge readers, physical keys, biometrics and key codes. Video cameras provide monitoring and recording of physical access. *Protiviti walked through the physical security controls in place to limit physical access to data centers and equipment rooms, obtained an understanding of the access approval and auditing process, and reviewed video monitoring capabilities.*

# Executive Summary (continued)

- **Backup and Recovery/Disaster Recovery Planning:** Ensuring essential data is frequently backed up and available for restoration is critical to restoring failed systems. Disaster recovery planning ensures that day-to-day business operations can be maintained during and after an unplanned event. *Protiviti evaluated the backup and recovery infrastructure and configuration for a sample of systems, disaster recovery site build-out and planning, procedures, and the recoverability of systems.*

- **Asset Management:** Maintaining an up-to-date inventory of equipment is required to support equipment life cycle management and strategic decision making for the IT environment. Additionally, many compliance programs require that equipment that stores or transmits sensitive data is inventoried and tracked by location. *Protiviti obtained an understanding of how data center assets are tracked and conducted a one-way inventory of select devices to assess the accuracy of documentation.*

- **Logical Access:** Logical access controls are the tools and protocols used for user identification, authentication, and accountability on IT systems and infrastructure devices. *Protiviti obtained an understanding of the access approval process and reviewed current access for select systems within the Port's data centers to determine if access was appropriate.*

# Highlights and Accomplishments

Although the focus of the audit was to identify areas of improvement within the Port's data centers, it is also important to note those areas where current processes are strong and infrastructure robust. The following is a list of positive areas, or commendations, that the Protiviti team would like to note for the benefit of the Port's management.

## Information Communication and Technology

- Staff are highly knowledgeable and skilled in their respective roles as they relate to the data center environment.
- The overall data center layout is designed in a manner that provides easy access to equipment and cabling. The new rack design that is being rolled out for new systems is clean, efficient and aligns with good data center design practice.
- A formal plan has been developed to improve the Disaster Recovery and Contingency Operations plans aligning with NIST 800-series standards.
- Standalone UPS systems have been installed in data centers as a stop-gap solution for the unreliable central UPS system.
- Leveraging a third-party data center site as a warm site provides an excellent site for contingency operations in the event the Port experiences a service impacting event.
- Formal policies and procedures have been developed to help guide the confidentiality, integrity, and availability of IT services and data center operations.

# Highlights and Accomplishments (continued)

## Aviation Maintenance

- Several critical infrastructure and applications maintained by Aviation Maintenance were configured with local redundancy via multiple data center locations in the airport to provide high availability for these systems.
- Staff appear to be well trained in their respective responsibilities and there is a large team of Electronic Technicians (ETs) in place to provide 24x7 support to the data center. Staff are highly knowledgeable and skilled in their respective roles as they relate to the data center environment.
- The new Access Control system installation was completed with proper power sourcing configurations, cable and equipment management, and defines a reliable design standard going forward.
- Standalone UPS systems have been installed in data centers as a stop-gap solution for the unreliable central UPS system.
- Generator testing is conducted frequently to ensure backup power can support data center operations under load and proactively detect potential issues.

# Summary Observations

The major observations identified by the Data Center Audit are listed in the following sections of the report. Although the Port has many well-designed processes and controls in place, we identified specific areas in which data center operations can be modified to improve the overall capabilities, availability and security of critical services. Protiviti noted the following themes throughout the Port's data centers:

- **Policies and procedures related to the day-to-day operations, maintenance, standards, and practices are divided between two separate groups and disciplines:** AV and ICT have separate policies, procedures, processes and standards for maintaining the ongoing operation of the Port's data centers. This can result in the inconsistent application of standards and practices in managing the data centers which can cause unforeseen incidents in the data center due to variation in processes and standards.

- **Data centers were not built for intended purpose:** The Port's data centers were not specifically designed to house and maintain IT equipment.

- **The Scheidt Bachmann parking revenue system backup procedures are insufficient:** The Scheidt Bachmann parking access and revenue control system is backed up to tape daily. However, it is stored in the same room as the Scheidt Bachmann system. If the data center were destroyed, the system and associated backup media would likely be destroyed. This could impact the Port's ability to recover the system within a reasonable time frame impacting revenues from parking garage operations during the downtime.

- **Aviation Maintenance has not created a formal Disaster Recovery Plan:** While Aviation Maintenance performs backups for critical systems, there has not been sufficient focus on the development of a comprehensive disaster recovery program. This would include the completion of a business impact analysis (BIA) to determine if the current process and capabilities are appropriate to meet businesses needs during an unplanned outage, documenting core recovery procedures for critical systems and conducting regular testing to validate system recoverability.