

# INTERNAL AUDIT REPORT

INFORMATION TECHNOLOGY AUDIT  
IT CHANGE MANAGEMENT

June 17, 2017 – October 30, 2017

ISSUE DATE: December 08, 2017  
REPORT NO. 2017-18

Prepared by Point B in partnership with the Port of Seattle Internal Audit department

## TABLE OF CONTENTS

EXECUTIVE SUMMARY .....	3
BACKGROUND .....	5
AUDIT SCOPE & METHODOLOGY .....	6
SCHEDULE OF FINDINGS AND RECOMMENDATIONS .....	9
APPENDIX .....	12
GLOSSARY .....	14

## EXECUTIVE SUMMARY

As part of the 2017 Port of Seattle Internal Audit Plan, Point B completed an audit of the Information and Communications Technology Department (ICT) IT Change Management process and tools for the period June 17, 2017 – October 30, 2017. The audit assessed ICT's controls for managing change to ICT's production applications and infrastructure. IT Change Management is not directly subject to external regulatory or financial control requirements; however, an ineffective change management process can result in downtime for critical business systems.

We found that ICT's IT Change Management process is clearly defined and well-practiced. The number of unplanned outages caused by IT changes is low and customers report very few significant disruptions despite a near-daily frequency of changes. These are both positive Key Performance Indicators. However, ICT management and staff recognize that additional process improvements, tools, and controls will reduce risk further. The audit identified two key opportunities for improvement:

- ICT's four independent service management applications lack the integration necessary to effectively manage and measure change across the Port's complex applications and infrastructure. IT Change Management Key Performance Indicators (KPIs) cannot be accurately measured. Collateral impacts to integrated systems might not be identified and mitigated in advance, resulting in unplanned business outages.
- ICT and Aviation Maintenance do not share common processes and tools to manage change in business systems that span the responsibilities of both organizations. Lack of a mutual approach to Change Management and a single source of record for system configurations greatly increase the risk of unplanned business disruptions. We recognize that this is currently not possible, but suggest this as a consideration for the long range plan.

We believe that the evidence obtained during the audit provides a reasonable basis for our findings and conclusions based on our audit objectives.

Management agrees with the issues and has developed action plans to remediate these issues. (See schedule of findings and recommendations in the attached document). We extend our appreciation to the management and staff of the Information & Communications Technology Department and to Aviation Maintenance for their assistance and cooperation during the audit.



Glenn Fernandes  
Director, Internal Audit  
Port of Seattle



Scott Watson  
Principal Consultant  
Point B

**RESPONSIBLE MANAGEMENT TEAM**

Peter Garlock, Chief Information Officer (CIO)

Matt Breed, Director ICT Infrastructure Services

Kim Albert, Director ICT Technology Delivery

Selena Tonti, Director Security and Preparedness

Lance Lyttle, Managing Director Aviation

Stuart Mathews, Director AV Maintenance

Gary Richer, Sr. Manager Aviation Maintenance

## BACKGROUND

The Port of Seattle Information and Communications Technology Department (ICT) provides enterprise technology services to all Port offices and facilities as well as the Port's tenants and guests. Services include the design, installation, operation, and support of custom and off-the-shelf business applications for the Port's business units, as well as the underlying technology infrastructure, information security, end user support, and project management.

IT Change Management governs the identification, prioritization, authorization, release, and communication of all changes to production technology environments. The process objectives are to:

1. Identify and quantify the risk and impact of changes to the production technology
2. Minimize both planned and unplanned business service disruptions
3. Manage the prioritization and release of change to production environments
4. Effectively communicate upcoming changes and disruptions to affected business stakeholders

ICT Personnel are required to adhere to the IT Change Management process for all changes to the Production and Pre-Production environments. Each week, proposed changes are recorded in an IT Change Management log, reviewed by key personnel from each IT discipline, discussed at the weekly Change Advisory Board (CAB) by all technical teams, and if approved are released into the production environment and communicated to customers. In the event of a sub-optimal or failed change, the CAB conducts a post-change review (PCR) the following week and the root cause of the failure is used to reduce future incidents.

ICT actively executes and enforces IT Change Management. The audit noted that management reinforcement of the process's importance is oral, documented by policy, and visual. For example, the policy is posted at the end of every equipment rack in the data center as a reminder. The process is engrained in the culture of the organization; it's a sign of a mature process and organization.

The ICT IT Change Management process manages approximately 1,700 changes annually.



*Figure 1. IT Change Management signage*

## AUDIT SCOPE & METHODOLOGY

### OBJECTIVE

The Port relies heavily on complex technology and information systems to manage its diverse operations and to drive success of its initiatives, strategies, and programs. As such, effective controls over information systems and related operations are critical to assure the integrity, reliability, and continuity of its business operations. The objective of this audit was to assess the appropriateness, efficiency, and effectiveness of ICT's IT Change Management process against the business requirements and industry best practices, and to validate that controls are appropriate to maintain the objectives of the process.

The audit included the following actions to meet those objectives:

- Determine if the existing process definition adheres to industry-accepted best-practices and frameworks
- Verify that ICT executes the process with sufficient diligence, management, and oversight to achieve the process objectives
- Determine whether the process controls are sufficient to monitor and maintain the process efficacy
- Assess whether ICT's process effectively meets the business requirements for volume and velocity of change
- Evaluate controls governing the use of normal, standard, and unscheduled change categories
- Review the appropriateness of the roles and responsibilities of the process owners and participants
- Determine whether effective integration is maintained between IT Change Management and three other key Service Management processes: Incident, Problem, and Asset
- Provide ICT with expert perspective on high-functioning IT departments, including real-world insight on how the Port's practices compare to similar organizations
- Where appropriate, identify pragmatic corrective actions to improve or maintain the existing process
- Customize the audit's level of specificity, testing, and reporting to the business requirements of the Port such that outcomes will best meet the needs and goals of the Port

Organizations typically leverage frameworks for best practice IT Change Management processes such as: ITIL, Control Objectives for Information and Related Technologies (COBIT), or International Standards Organization (ISO) Frameworks provide. While these frameworks outline critical components of service management processes, they are not specifically directive and organizations are expected to adapt the framework to their individual business requirements. The audit considered these differences. ICT uses ITIL as their primary framework for developing processes.

**IN-SCOPE:**

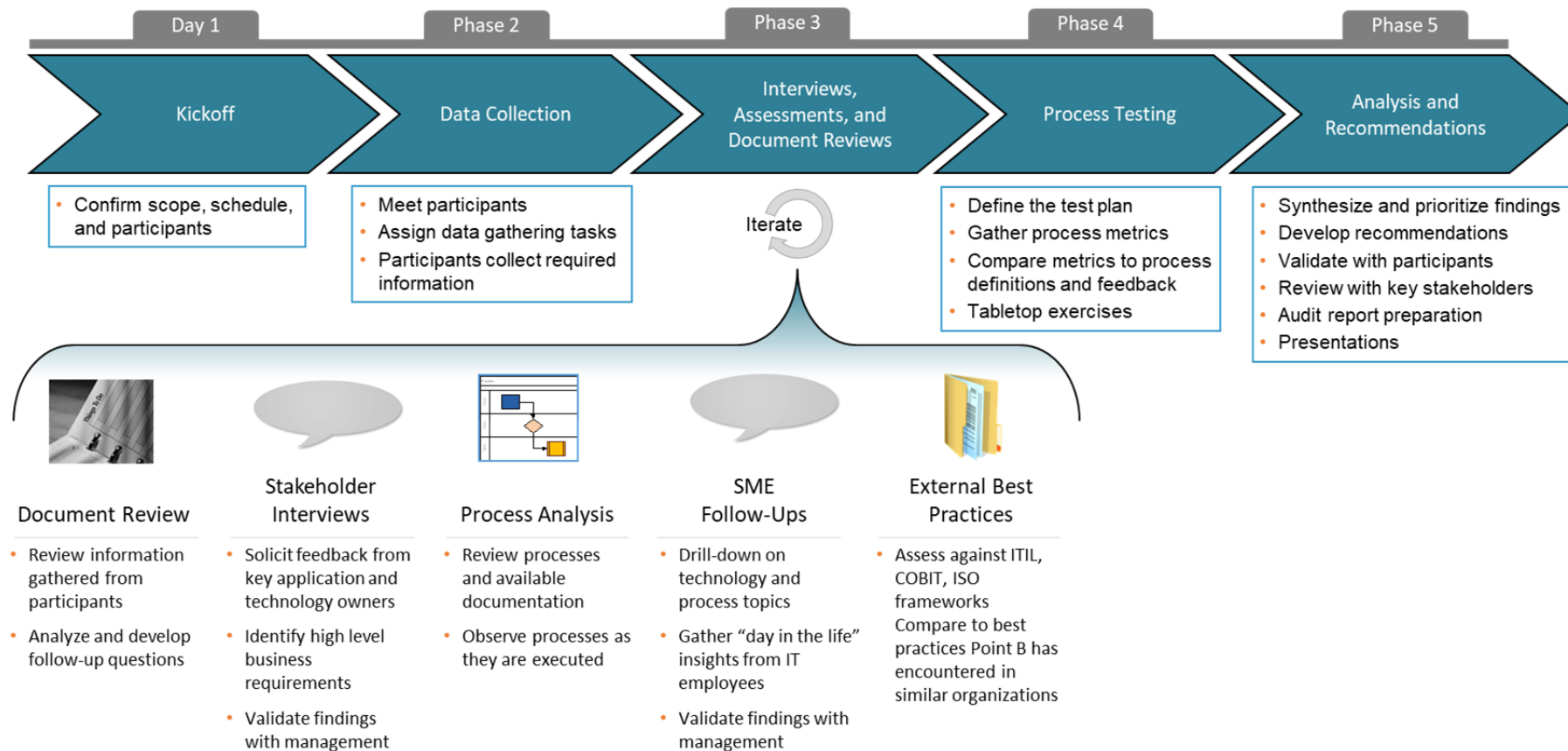
- ICT's IT Change Management process
- Process hand-offs and interfaces to other critical service management processes, specifically Incident, Problem, and Asset Management
- Roles and responsibilities of the process owners
- Existence and effectiveness of the process controls
- Changes executed between July 1, 2015 and June 30, 2017

**OUT-OF-SCOPE:**

- Audit of Incident, Problem, and Asset service management processes
- Substantive testing of financial impacts – IT Change Management does not have fiscal component and does not impact accounting or financial statements
- IT Change Management practices of non-ICT departments, such as Aviation Maintenance (Electronics Technicians), except as to gather their insight as participants in the ICT process

## APPROACH

The following diagram outlines the audit approach. Point B, an external management consulting firm, conducted this audit under the oversight of Port of Seattle’s Internal Audit department. Point B has been engaged to augment Internal Audit with deep expertise in the people, process, and technology aspects of IT Change Management.





## SCHEDULE OF FINDINGS AND RECOMMENDATIONS

### 1) RISK RATING: MEDIUM

ICT's four independent service management applications lack the integration necessary to effectively manage and measure change across the Port's complex applications and infrastructure. IT Change Management Key Performance Indicators (KPIs) cannot be accurately measured. Collateral impacts to integrated systems might not be identified and mitigated in advance, potentially resulting in unplanned business outages.

ICT maintains several self-developed and purchased applications for managing IT services. The IT Change Management process uses a Microsoft SharePoint and InfoPath tool to record and approve changes. IBM's Maximo application is used to manage incidents and service requests and some change requests. Assets are tracked in the PeopleSoft financials application. Relationships between applications, servers, and storage are recorded in a custom-built Application Catalog. While each tool supports the basic functions for the process it serves, a mature ITIL service management implementation requires a fully integrated toolset.

During the audit, several basic IT Change Management Key Performance Indicators could not be measured. The audit attempted to calculate these using extracts from each of the source systems, but could not due to insufficient data and data relationships between systems. These KPIs included:

1. Change success rate (successful changes as a percentage of total changes)
2. Number of failed changes
3. Number of changes that caused unplanned business disruptions
4. Percentage of changes with incomplete or incorrect impact assessments (applications affected that were not identified ahead of the change)
5. Number of configuration discrepancies found as a result of changes
6. Frequency of major incidents and unplanned outages by type of change and severity of customer impact

Key root causes included:

1. Lack of standardized coding practices and data structures between the IT Change Management tool, Application Catalog, Maximo, and PeopleSoft applications
2. The IT Change Management process only governs changes entered into SharePoint; Maximo changes are not reviewed
3. Maximo incidents do not identify the specific change that caused the service disruption
4. Maximo identifies persons impacted by a failed change, not the application that failed

ICT has adopted the industry-best-practice ITIL methodologies developed by the British government to maintain effective service levels. ICT's processes are mature and practiced, but not supported with adequate tooling. In order to continue to be effective, a new integrated service management toolset is required – one that is built for ITIL methodologies and capable of addressing the Port's complex technology environment.

**Recommendation**

1. Initiate a project to replace the existing independent tools with a single, integrated service management application
2. Adapt the existing IT Change Management process to take advantage of the new service management toolset
3. Assign responsibility for regularly measuring and communicating IT Change Management Key Performance Indicators
4. Develop process controls and measures for maintaining the accuracy of the configuration data supporting IT Change Management

**Management Response:**

Management agrees with the assessment and recommendations.

A new toolset has already been selected and a project has been initiated with an estimated completion of initial deployment by March 31, 2018. KPIs, process controls and measures will follow the initial deployment and are expected to be completed by June 30, 2018.

## 2) RISK RATING: MEDIUM

ICT and Aviation Maintenance<sup>1</sup> do not share common processes and tools to manage change in business systems that span the responsibilities of both organizations. Lack of a mutual approach to IT Change Management and a single source of record for system configurations greatly increase the risk of unplanned business disruptions.

The Port of Seattle's business units rely on a web of tightly-integrated systems supported by Information & Communication Technology (ICT) and Aviation Maintenance. ICT leverages a formal change management process and toolset, based on ITIL best practices, that has been in place for approximately 8 years. Aviation Maintenance leverages ICT's process and tools for changes that impact the financial systems, but the organization has an independent process to support change management on other applications. Both organizations agree that opportunities exist to share practices, tools, and information in order to jointly reduce the risks of unplanned business disruptions.

Industry best practices recommend that all Information Technology departments in an organization use a shared set of Service Management processes and tools. This allows individual IT teams to identify cross-system dependencies, engage their counterparts for insight, increase communication and coordination during changes, and reduce unplanned business disruptions. We realize that in the immediate term, using a shared set of Service Management processes and tools is unrealistic. However, due to the importance of Change Management and the impact it can have on critical systems, Internal Audit will recommend that the organizations consider this for their long range plan. Additionally Internal Audit will independently review the Aviation Maintenance Change Management process in 2018.

### Recommendation

1. We recommend that the two organizations leverage off each other to identify shared tools and processes that can be used across both organizations to improve service management.

### ICT Management Response:

ICT Management agrees with the rating and recommendation.

### Aviation Maintenance Management Response:

Aviation Maintenance Management would like to invite the Audit Team to review the Electronic Technicians Change Management System. We believe this would provide aviation maintenance staff with input on how well the aviation Maintenance Change Management System process is functioning, and to provide input to ensure aviation maintenance processes are consistent with industry best practices. As ICT moves forward to upgrade their current Change Management system, aviation maintenance would like to participate from the beginning to determine if any new processes would also meet the needs of the entire organization, and provide a standard Change Management System for the two departments.

---

<sup>1</sup> Aviation Maintenance was out of scope for this audit, however, this finding and the related risk, impacts both ICT and Aviation Maintenance and requires both parties to partner to develop a uniform process.

## APPENDIX

## 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
<b>HIGH</b>	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
<b>MEDIUM</b>	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
<b>LOW/ Exit Items</b>	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

## APPENDIX B

### GLOSSARY

**Information & Communications Technology (ICT)** – An enterprise Information Technology department within the Port of Seattle.

**ITIL** - a set of detailed practices for IT service management (ITSM) that focuses on aligning IT services with the needs of business. Originally developed by the United Kingdom Cabinet Office, ITIL is recognized as a best-practice methodology across most industries.

**Change Advisory Board (CAB)** – A group of individuals and a forum for reviewing and approving (or denying) proposed changes. At the Port, the CAB meets Tuesday afternoons to review and approve the changes scheduled for the next seven days. The CAB includes a senior engineer from each of the ICT technical disciplines and the meeting is led by the ICT Service Desk manager.