Enterprise Technology Risk and Performance Assessment

Port of Seattle®

December 2012

Powerful Insights.
Proven Delivery.®

protiviti®
Risk & Business Consulting.
Internal Audit.

Executive Summary: Introduction

✓ At the request of the Port of Seattle Commissioners and Executive Team, Protiviti was engaged to conduct an Enterprise Technology Risk and Performance Assessment.

✓ The project was initiated in the September 2012 timeframe and was completed and finalized in December 2012.

✓ The scope consisted of Port technology organization wide and included both the Information Communication & Technology (ICT) and Aviation Maintenance departments.

✓ The project consisted of two primary objectives:

1. Execute a technology risk assessment resulting in a thee-year IT Audit plan, including direction on staffing levels and appropriate skills sets to complete the recommended audits.

2. Assess the overall management, efficiency and effectiveness of Port information and communication technology assets and services within the following key areas: Strategy, Operations, Investment, Governance and Risk Management

✓ This report encompasses the analysis, conclusions, observations and recommendations derived by Protiviti as a result of the procedures it performed.

✓ Procedures performed included a broad set of interviews with organization leadership and process leads; reviews of provided policies, procedures, and process documentation; and detailed benchmarking analysis.

protiviti®

Executive Summary: High-Level Observations

✓ Technology is rapidly changing and absolutely critical to the Port's overall operations.

✓ Properly aligned technology capabilities are essential to enhancing the efficiency and effectiveness of the Port's business processes through the protection, reliability, availability, and analysis of business information.

✓ IT cost benchmarking analysis conducted by Protiviti indicates the Port's IT functions have effectively managed costs, including the following key results:

- The Port's IT cost profile is in alignment with comparable industry averages.

- The Port has generally outperformed comparable industries in controlling IT operations (or "run") costs.

- The Port has successfully shifted more of its IT spend towards growth and transformation of the business from maintaining legacy infrastructure and applications.

✓ The Port's IT processes perform favorably compared to organizations of comparable size and industry-groups.

protiviti®

Executive Summary: High-Level Observations (continued)

✓ Opportunities exist to:

- Further mature certain core IT processes.

- Continue to align ICT and Aviation IT operations.

- Explore additional avenues for collaborating and communicating with the Commission and C-Level positions.

protiviti®

Executive Summary: Key Observations & Recommendations

IT Governance & Alignment

- The Port's ICT Governance Board provides effective oversight to major IT initiatives and decisions, including investment evaluation / prioritization and risk management.

- Business units should initiate regular formal strategy discussion and alignment review processes with the IT functions where they are not in place today.

- Aviation should continue the close alignment of its technology decision-making and communication processes with the ICT Governance Board.

- IT leadership does not regularly interact with the Port Chief Executive Office (CEO) or Commissioners.

- The Port IT functions should establish consistent processes and responsibilities focused on strengthening and continuously managing the relationship with IT's business customers.

IT Value & Cost Perception

- Aviation and Corporate functions require (and receive) a more sophisticated set of IT solutions which require a more sophisticated IT function to deliver.

- Other divisions, while not requiring as sophisticated a set of solutions are still benefiting from a high performing IT function.

- The basic model for allocating IT costs to business units is generally fair (based on system usage), some of the "lighter" users of IT perceive their allocated share to be excessive.

- Peer group and performance benchmarking indicate the overall size and cost of the Port's IT function are consistent with the Port's IT objectives. No cost cutting efforts are recommended.

protiviti®

Executive Summary: Key Observations & Recommendations (continued)

IT Operational Capabilities, Process Maturity & Alignment

- The Port IT organization has established a core set of IT processes and capabilities that enable consistent delivery of IT services.

- The Port should continue to invest in improvements to its IT process, technological, and organizational capabilities including: (1) upgrades to specific data center facilities, (2) expanding the IT security organization, (3) enhancing and maturing IT service continuity processes, and (4) improving the IT service support processes and systems (including change management and service level management).

- The Port should continue to align and adopt common processes across IT functions, leveraging the existing ICT processes since they have more established practices and structures and also demonstrate higher levels of maturity.

IT Project Intake & Analysis

- The Port has demonstrated strong execution capabilities for IT projects and investments that are initiated through the ICT Governance Board and IT project management organizations.

- The Port should establish an enterprise-wide IT architectural review process that is required for all projects with potential IT implications, closely integrating with the existing ICT Governance Board and the Airport Technology Investment Committee.

protiviti®

Executive Summary: Key Observations & Recommendations (continued)

IT Internal Audit Function

- The Port does not have a formal IT audit function with the specific skill sets necessary, which limits its ability to independently assess IT risks.

- The Port should establish an IT audit planning process within its Internal Audit Department.

- Audit efforts should be closely coordinated with both ICT and AV to ensure scheduling aligns with other IT initiatives and that resources are available.
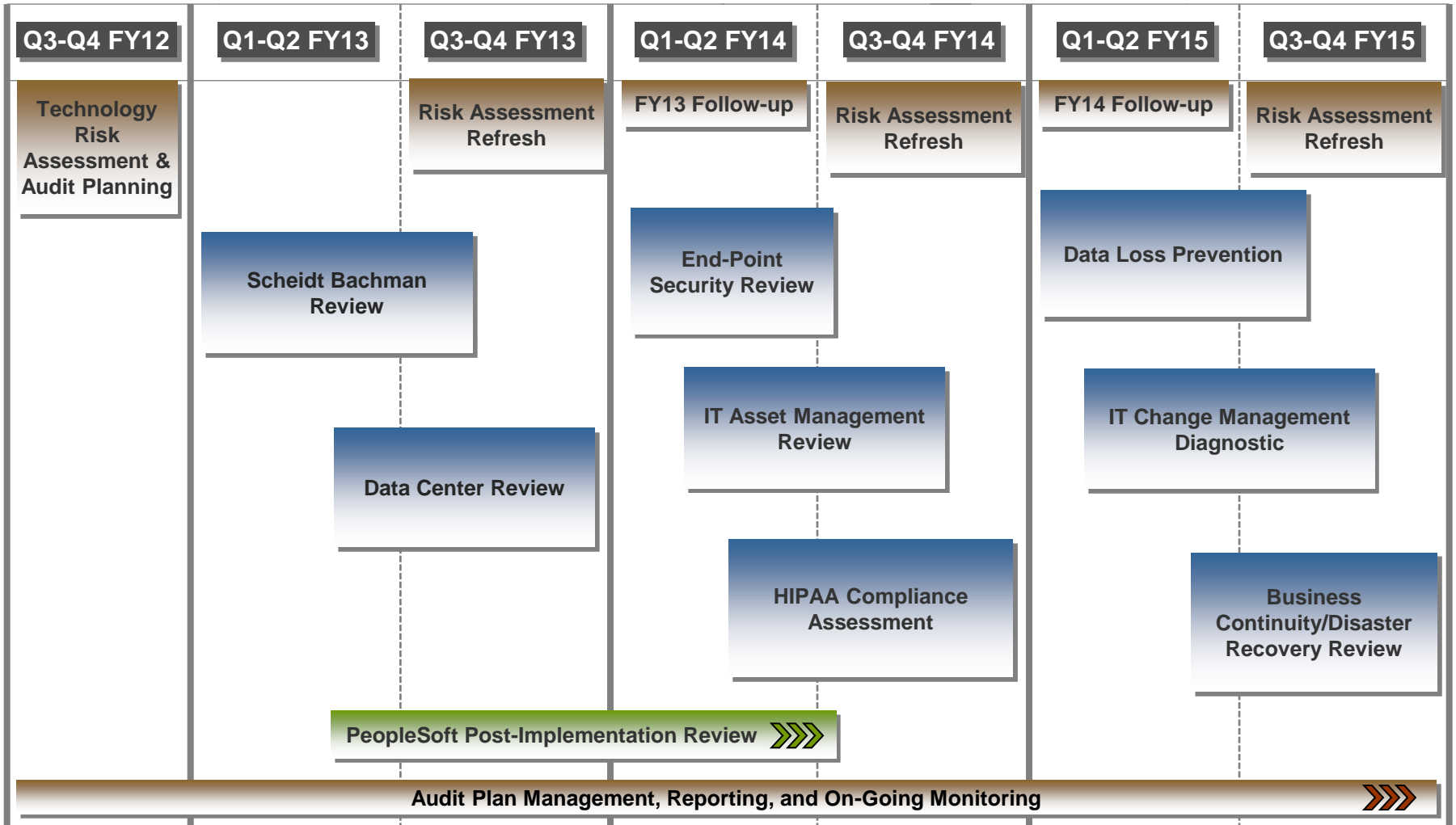
protiviti®

Technology Risk Assessment

IT Risk Assessment Approach

IT Risk Assessment				

Key Stakeholders Interviews / Document and Data Requests		Management Input and Oversight		Management Review and Approval

Project Phases

Understand IT Organization and Structure	Understand IT Environment	Determine Risk Universe	Prioritize Risk Universe	Finalize IT Audit Plan

Key Inputs

Understand IT Organization and Structure	Understand IT Environment	Determine Risk Universe	Prioritize Risk Universe	Finalize IT Audit Plan
IT Org Charts	Applications	Key IT Projects	CobiT / ITIL / ITPI	Risk Universe
Geographic Locations	Infrastructure	Processes	Capability Maturity Model	Audit Hours / Timeline
Budgets	Voice / Data Networks	Departments	Perceived Risk	Audit Scope / Objectives
Business Interaction	IT Operations	Applications / Infrastructure	Protiviti Experience	Required Audit Skills
	Data Center			

Project Management	Knowledge Sharing	Communication

protiviti®

Proposed IT Audit Plan

Q3-Q4 FY12	Q1-Q2 FY13	Q3-Q4 FY13	Q1-Q2 FY14	Q3-Q4 FY14	Q1-Q2 FY15	Q3-Q4 FY15

Technology Risk Assessment & Audit Planning

Risk Assessment Refresh

FY13 Follow-up

Risk Assessment Refresh

FY14 Follow-up

Risk Assessment Refresh

Scheidt Bachman Review

End-Point Security Review

Data Loss Prevention

Data Center Review

IT Asset Management Review

IT Change Management Diagnostic

HIPAA Compliance Assessment

Business Continuity/Disaster Recovery Review

PeopleSoft Post-Implementation Review ⟫⟫

Audit Plan Management, Reporting, and On-Going Monitoring ⟫⟫⟫

Audit Planning and Follow-up	**Audit projects**	**On-going Projects**

protiviti®

Technology Performance: Benchmarking & Metrics Analysis

protiviti ®

Benchmarking Results

Benchmarking Comparisons

Protiviti utilized three data points to benchmark the Port's information technology functions across similar organizations:

1. The IT Process Institute's **IT Controls Performance** which includes comparison data points on organizational size and IT control effectiveness.

2. The IT Process Institute's **IT Strategic Alignment Benchmark** which includes comparison data points on IT strategy models and alignment practices.

3. Gartner's **IT Metrics: IT Spending and Staffing Report** for a comparison of IT metrics across a variety of industries. The 2012 version of this report was used in conjunction with prior year reports for multi-year comparisons.

protiviti®

Benchmarking Results

Key Themes

Alignment with Key IT Metrics: The Port's IT metrics compare favorably with the North American and comparable industry averages (per analysis of key IT metrics from Gartner).

- ✓ Variations in metrics are within an acceptable margin of the comparable industry averages.

IT Strategic Focus: Business needs indicate the primary strategic focus of the Port's IT functions should be on partnering with the business to enhance processes in a "Process Optimizer" model. The core IT practices to enable this level of alignment are in place (per the ITPI Strategic Alignment Benchmark).

- ✓ The need for the "Process Optimizer" alignment model is being driven by the expectations of the two largest consumers of Port IT services: Corporate and the Aviation Division.

- ✓ The "Process Optimizer" model also effectively provides for the services required by other Port divisions desiring a lower level of IT alignment (e.g., in a "Utility Provider" model); however, the Port's cost allocation methodology may require revision to more accurately reflect the different divisions' IT expectations and utilization levels.

protiviti®

Benchmarking Results

Key Themes (continued)

IT Process Performance: The Port's IT processes activities perform as well as or better than organizations of comparable size and industry-groups (per the ITPI IT Control Performance Benchmark).

- ✓ The Port rates as a "High Performer" with two thirds of its measured IT performance metrics rating better than the benchmark average.

- ✓ The Port may realize additional performance gains (against the benchmark peer groups) with targeted improvements to the 12 "foundational" IT process activities.

Benchmarking Updates: The Port should consider revisiting these benchmarks every 2 to 3 years.

protiviti®

Capability Maturity Analysis

IT Capability Maturity Analysis Summary

Current Demonstrated Maturity State: **Repeatable to Defined**

Target Maturity State (1-3 Years): **Defined***

	Change, Configuration & Release Management	Continuity Management	Program, Project and Portfolio Management	Security Management	Support / Service Desk	IT Governance
Optimizing $$$						
Managed $$						
Defined $	Partial		Current		Current	Partial
Repeatable $$	Current	Partial	Current	Current	Current	Current
Initial $$$	Current	Current	Current	Current	Current	Current

Potential for increased costs is accepted to ensure process consistency & quality

Typical Target Zone: Cost & performance management are effectively balanced

Likelihood of increased costs due to process issues & inconsistency

* Note: Higher levels of maturity may be identified as the "best fit" option once the "Defined" level is consistently achieved by the Port.

Legend: Current Maturity (gray) — Partial Demonstration (yellow) — Target Maturity (green line)

Capability Maturity Model Matrix Example

Change, Configuration and Release Management (includes SDLC)

	Strategy & Policies	Processes & Controls	People & Organization	Management Reports	Methodologies	Systems & Data
Optimizing	Close alignment of change, configuration, and release (CCR) practices with business strategy; new initiatives are agile and successful	CCR processes are formally enforced, automated, monitored statistically, and are proactive (i.e., "near misses" identified)	Matrixed functions / roles adjust quickly to initiatives; ownership, roles, standards and cross-training are inherent in operations	World-class process performance; all changes are "normal"; system outages are rare and well-planned	Costs / benefits / risks measured and balanced in portfolio of changes, releases, and projects across infrastructure	Real-time system controls prevent service interruptions; excellent data integrity; automated config. data prevalent
Managed	CCR policy / objectives ingrained into IT governance practices; service measures designed into process	CCR processes are integrated; enforced by some preventive controls; monitoring capability exists	CCR ownership / roles evident; cross-training limits failure points; config. teams support multiple Bus	Management by exception; few (<1%) emergencies / failures; config. data proactively managed	Process performance benchmarked to plan for future; config. integrated with other IT processes	Integrated change process systems; "Real-time" trending; Integrated CMDB with automated detection
Defined	Policy and strategy define objectives for success; policy emphasizes that "no unauthorized changes" are made	Practices understood, but largely manual; releases include rollback plans; config impact analysis In place; detection of failures is unlikely	CCR roles defined; process ownership clearly established; process awareness widespread; some cross-training; CAB includes business	KPIs analyzed periodically; service thresholds in place; success measured in terms of ROI/TCO; infrequent (<2%) emergencies/failures	Models include impact analysis & risk mitigation activities; IT process integration beginning; history of changes is traceable (e.g., at CI-level)	1-2 primary systems used to manage changes; reporting structures defined / available; CMDB in place with some data collection automation
Repeatable	Basic policy exists to establish authority and responsibility; limited long-term strategy and vision; informal planning	Change / release process is somewhat consistent; informal enforcement / training; config. process definition beginning	Some responsibilities understood; limited training available; CAB established but with only IT; some config. coordination	Few metrics defined; data gathered through periodic audits; somewhat frequent (≤10%) emergencies / failures and change-related outages	Basic models are considered, but used inconsistently; mass "data changes" are normal; limited view of configurations	Some auto-data collection, but with manual input; config. data manually held; segregated test environments exist
Initial	No strategy or policy for managing change to IT systems exists	Processes are informal, differ significantly between groups, and are adjusted reactively	Change success results from heroics and responsibility not consistent; siloed config. Knowledge	Only anecdotal evidence available; frequent (>20%) emergencies/failures; frequent change-related outages	Process not defined as "request to close"; siloed processes; config. relies on "expert knowledge"	Manual or redundant data gathering; accurate config. data unavailable; changes often cause issues

increased Costs (Optimizing–Managed)

Typical Target Zone (Defined)

increased Costs (Repeatable–Initial)

Legend:
- Current Maturity (gray)
- Partial Demonstration (yellow)
- Target Maturity (green line)

Powerful Insights.
Proven Delivery.™

Confidentiality Statement and Restriction for Use

"This report (i.e., report of findings/recommendations, table, chart, summary, etc.) provides management with information about the condition of the Port of Seattle's environment at one point in time. Future changes in environmental factors and actions by personnel may significantly and adversely impact these in ways that this report did not and cannot anticipate. This report is intended for use by Management, solely for the purpose of providing direction to its internal. It is not to be used or relied upon by others for any other purpose whatsoever. "

protiviti®