Enterprise Technology Risk and Performance Assessment

Port of Seattle

December 2012

Powerful Insights.
Proven Delivery.®

protiviti®
Risk & Business Consulting.
Internal Audit.

Table of Contents

protiviti®

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 time frame 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.

Executive Summary: Procedures Performed

- ✓ Conducted interviews with key IT and business leads including leadership from the Airport, Seaport and Real Estate divisions, as well as corporate and the audit committee.
- ✓ Requested and reviewed documentation related to core processes, upcoming projects, application inventory, infrastructure, service level agreements, budgets (including budget projections and allocations,) risk management, risk assessments, strategy and operations.
- ✓ Gathered key data points for benchmarking purposes using Gartner and IT Process Institute (ITPI) research sources.
- ✓ Refined benchmarking results to better align with Port's organizational structure and industry.
- ✓ Compiled a technology auditable universe and risk ranked those elements based on key criteria (e.g., impact on strategy, operations, regulation, etc.).
- ✓ Established a three-year IT audit plan based on the IT audit risk ranking exercise.
- ✓ Based on the overall analysis resulting from both the IT Risk Assessment and performance benchmark, documented key observations and recommendations for enhancing overall process and technology maturity and improving organizational interactions.

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.

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 discussions 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 in turn require a more sophisticated IT function to deliver them.
- 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 also 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.
- Going forward, the Port should establish its own 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

protiviti®

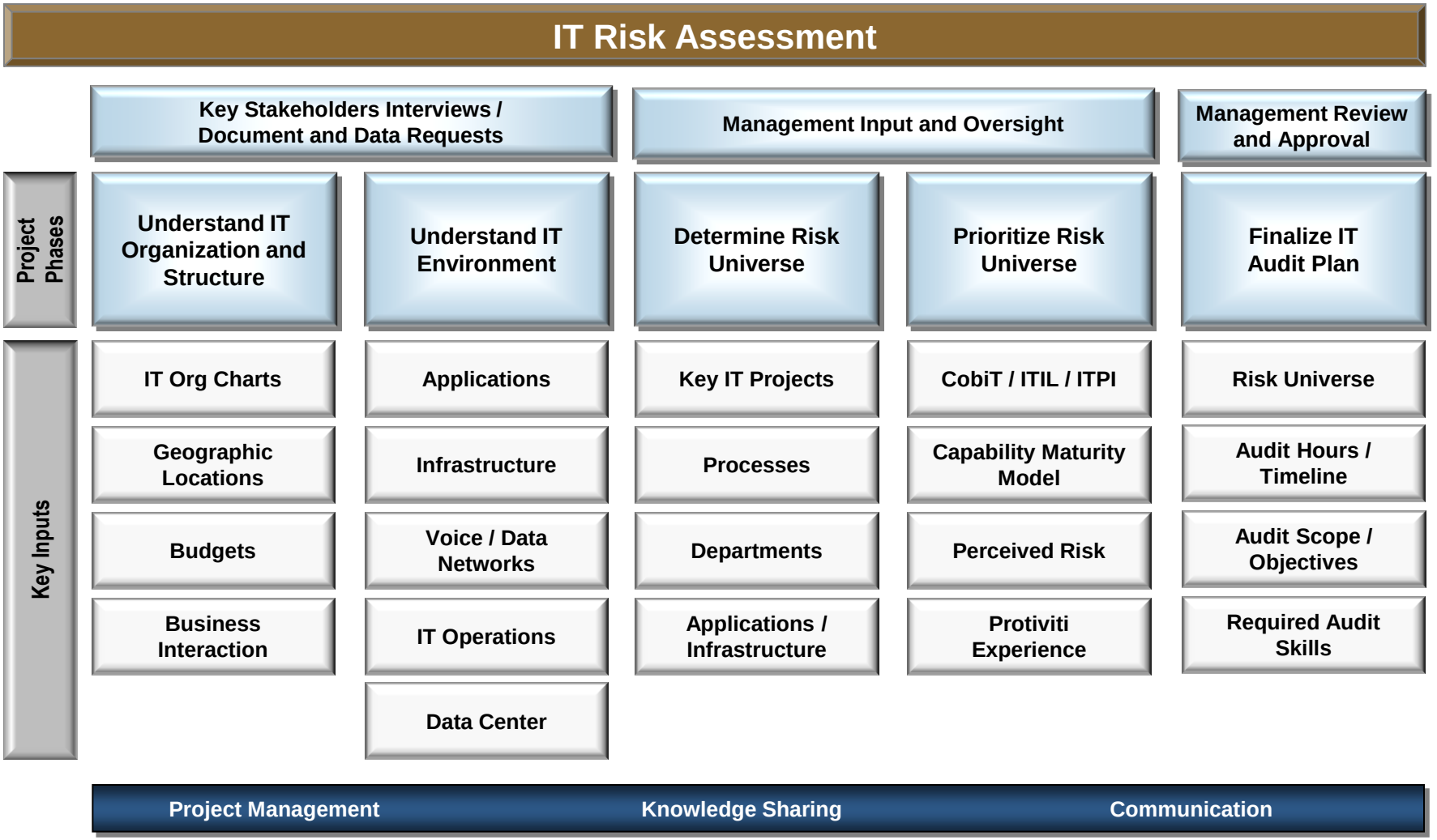
IT Risk Assessment Approach

IT Risk Assessment

- ✓ The IT risk assessment approach, as presented on the slide that follows, is built on the foundation of Protiviti's Technology Risk Model and uses this framework to identify the universe of potential auditable areas (the risk universe) within an organization's technology footprint.
- ✓ This model utilizes commonly used IT internal control frameworks such as ITIL (IT Infrastructure Library) and CobiT (Control Objectives for IT) to help identify and narrow down the list of potential IT audits.
- ✓ To ensure the effectiveness and accuracy of the process, management involvement and oversight is required through out the effort.
- ✓ The goal is to identify all of the different factors affecting the IT environment and risk rank them appropriately.

protiviti®

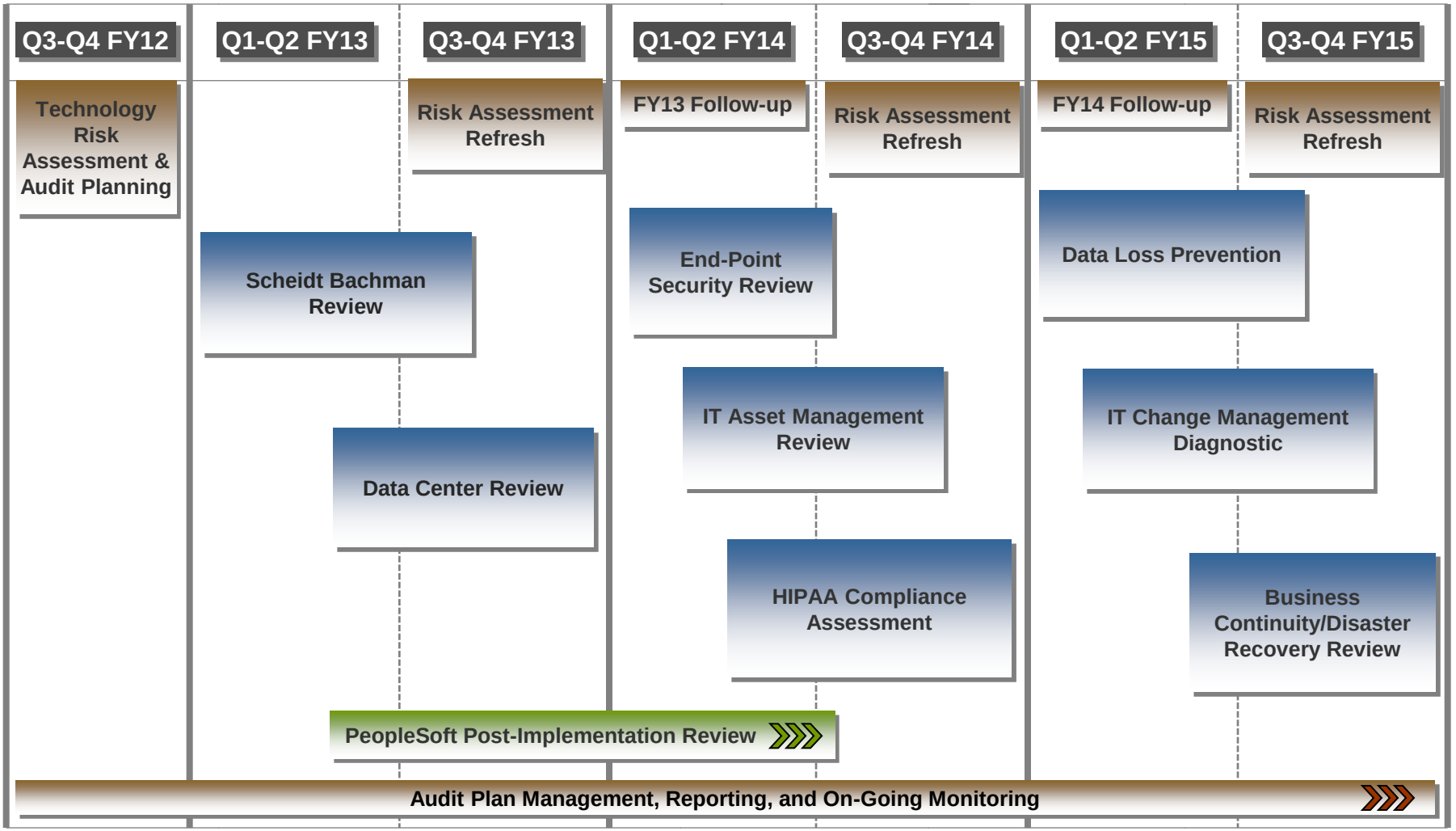
IT Risk Assessment Approach (continued)



Technology Risk Universe

- ✓ The IT Risk Universe matrix, located in the appendices of this report, is populated with the individual IT elements identified within the Port's IT environment.
- ✓ The risk universe elements were determined through the following sources:
  - Topical areas of interest based on interviews performed and documentation received from various Port sources
  - Data and information derived from the performance benchmark efforts
  - Protiviti experience and methodology
- ✓ Once the IT Risk Universe was populated with the various IT elements, they were categorized as a component, process, application or project as it relates to the IT environment:
- ✓ Protiviti then rated each risk based on its impact to the following criteria:
  - Strategic / Planning
  - Organization / Operations
  - Service / Marketplace
  - Financial
  - Regulatory / Legal Exposure
  - Data Integrity / Information
- ✓ A raw risk rating for each risk was calculated based on the criteria above assuming that internal controls are not in place.
- ✓ We then calculated the final residual risk rating taking into account the strength of the internal control environment. Considerations for the internal control environment rating included results of the performance benchmarks (i.e., maturity of processes), strength of team, focus and level management oversight and focus.
- ✓ The 3 year IT Audit plan is provided on the following slide.

Proposed IT Audit Plan



protiviti®

High-Level IT Audit Project Scopes

The tables below outline the suggested IT audits for 2013, 2014 and 2015 along with the recommended scope of effort, suggested skill sets to execute the review and estimation of necessary hours to complete.

2013 IT Audit Plan			
IT Audit	**Recommended Effort**	**Suggested Skill Sets**	**Estimated Hours**
PeopleSoft Post-Implementation Review	• Conduct a post implementation review 1 to 3 months after go live • Analyze business and IT requirements and verify that the implemented solution aligns with those original expectations. • Verify that testing procedures and controls adequately mitigate risk around the system implementation. • Ensure that core IT general controls were considered and applied to the implemented solution. • Review developed roles within the implemented solution to ensure that segregation of duty risks have been identified and addressed. • Note: Protiviti would normally recommend a detailed review prior to go live. However, constricted project timelines and the ability to quickly engage an appropriate party to execute the review may introduce additional risk to the effort.	• Experience with ERP implementations (PeopleSoft preferred.) • Good understanding of the following: – Project risk Management – SOD configurations – Native PeopleSoft control configurations – Data Migration and Testing Strategies – SDLC	250 to 300 hours

protiviti®

High-Level IT Audit Project Scopes (continued)

2013 IT Audit Plan			
IT Audit	**Recommended Effort**	**Suggested Skill Sets**	**Estimated Hours**
Scheidt Bachman Parking System Review	• Working with a cross functional Port team support a detailed analysis and review of the current Scheidt Bachman install. • Determine whether core controls are in place and whether they're operating effectively in the following areas: – Security: System is protected against unauthorized access (both physical and logical). – Availability: System is available for operation and use as committed and agreed, – Data integrity: System processing is complete, accurate, timely and authorized. • Support substantive testing efforts. • Note: the team may also draw upon any PCI testing efforts involving the system.	• Understanding of application architecture • Strong information security skills (CISSP preferred.) • Strong IT audit skills (CISA preferred.)	250 hours

protiviti®

High-Level IT Audit Project Scopes (continued)

2013 IT Audit Plan			
IT Audit	**Recommended Effort**	**Suggested Skill Sets**	**Estimated Hours**
Detailed Data Center Review	• Review will cover all in scope data centers • Review all policies and procedures and other documentation associated with the management and design of the data center. • Assess the redundancy, maturity, and stability of physical, logical, and environmental controls within the data center. • Determine monitoring and response capabilities of IT within the data center environment. • Review and comment on current data center strategy. • Identify design and management gaps. • Verify the ability of the data center locations to perform as a recovery sites in the event of a disaster.	• Clear understanding of Data Center design and architecture. • Knowledge of data center control best practice around the following: – Physical security – Infrastructure Monitoring – HVAC and environmental management – Power management and redundancy – Capacity & Change Management – Preventative Maintenance	200 hours

protiviti®

High-Level IT Audit Project Scopes (continued)

2014 IT Audit Plan			
IT Audit	**Recommended Effort**	**Suggested Skill Sets**	**Estimated Hours**
End Point Security Review	• Review policies and procedures associated with the management of end-user devices. • Document and assess controls associated with laptop encryption, firewalls, anti-virus, patch management, and PDA / Blackberry / iphone security, etc. • Assess current toolsets utilized for managing lost to stolen end point devices. • Review and comment on end point security strategies.	• Information Security Certified (CISSP / CISA preferred) • Solid understanding of encryption and available end point security products.	200 hours
IT Asset Management Review	• Document and evaluate the IT asset management process to determine overall effectiveness of cross-organizational IT group's ability to manage IT assets. • Evaluate the IT procurement process and associated controls. • Assess the overall maturity of the IT asset management procedures using industry leading practices (e.g., ITIL) as a comparison point. • Review Maximo and related work flows to validate its effectiveness relative to the Port's asset management lifecycle process.	• Understanding of asset management lifecycle and related toolsets. • ITIL Foundations or Practitioner Certifications	300 hours

protiviti®

High-Level IT Audit Project Scopes (continued)

2014 IT Audit Plan			
IT Audit	**Recommended Effort**	**Suggested Skill Sets**	**Estimated Hours**
HIPAA Compliance Assessment	• The scope of this assessment includes those systems and network elements at the Port that store, process or transmit credit Personal Health Information (PHI) including the support processes, system documentation, and system configurations related to compliance efforts. • Obtain an clear understanding and document the data flow of how PHI is collected, stored, and protected at the Port. • Scope the PHI environment to ensure all of the relevant systems and devices are considered. • Assess existing processes and controls in place to protect PHI against the HIPAA Security Rule to determine level of compliance and identify areas of improvement. • Test relevant controls to assess operating effectiveness of required controls.	• Personnel with experience evaluating and interpreting the HIPAA Security Rule of 1996 and HITECH. • Strong IT Audit and Information Protection skills (CISA, CIPP)	300 hours

protiviti®

High-Level IT Audit Project Scopes (continued)

2015 IT Audit Plan			
IT Audit	**Recommended Effort**	**Suggested Skill Sets**	**Estimated Hours**
Data Loss Prevention Assessment	• Identify relevant regulations and privacy laws related to the handling and protection of sensitive data at the Port such as: (1) Current state Privacy Laws, (2) Relevant federal regulations and industry guidance including HIPAA (note: credit card data will be addressed as part of the PCI review.) • Review all current policies and procedures related to the protection of PII. • Review data handling procedures for relevant departments to determine the following: (1)Types of data being collected, (2) How data is being collected and retained, (3) Retention formats (e.g., hard copy, electronic), (4) How long collected data is retained, (5) How retained data is protected, (6) How data is purged, deleted, or disposed of. • Identify all applications, databases and data stores where PII is being collected and/or stored. • Employ automated DLP tools to scan (1) data in motion within the organization and (2) data at rest on a sample of key company file shares.	• Information Security Certified (CISSP / CISA preferred) • Certified Information Privacy Professional (CIPP) • Experience ins the use of standard DLP tools (e.g., Vericept, Symantec, Websense, etc.)	300 hours

High-Level IT Audit Project Scopes (continued)

2015 IT Audit Plan			
IT Audit	**Recommended Effort**	**Suggested Skill Sets**	**Estimated Hours**
IT Change Management Diagnostic	• Review change management processes, identifying current risks and control gaps. • Gain a detailed understanding of the organizational reporting structure and key approval positions. • Identify all core applications and systems for which access is tracked and/or that follow the current change control process. • Document a detailed data flow chart describing the current approach by which changes are tracked, tested approved, deployed, etc. • Document an approval matrix establishing the appropriate levels and positions responsible for approving user access and changes to Port's IT environment. • Identify general efficiency gaps in the current processes as well as unmitigated risks and control weaknesses. • Assess Segregation of Duties configurations for critical systems (e.g., developer access to production).	• Experience auditing change control processes. • Detailed understanding of ITIL / Cobit frameworks and best practice guidance for Change Control process. • Strong IT audit skills (CISA preferred)	250 hours

protiviti®

High-Level IT Audit Project Scopes (continued)

2015 IT Audit Plan			
IT Audit	**Recommended Effort**	**Suggested Skill Sets**	**Estimated Hours**
Business Continuity / Disaster Recovery Review	• Assess the overall maturity of the business continuity program and to determine whether proper development and maintenance processes are in place as dictated by standard BC best practices. • The scope of the review should include evaluating and testing (where appropriate) the processes and documentation over the following aspects of the business continuity program: – Crisis Management – Crisis Communication – Training and Awareness – Plan Testing Elements – Plan Maintenance Activities – Disaster Recovery (IT) Planning – Business Process Recovery Planning – Risk Assessment execution – Business Impact Analysis (BIA) execution – Strategy Planning	• Clear understanding of common business continuity frameworks (e.g., Business Continuity Institute, Disaster Recovery Institute International, etc.) • Certified Business Continuity Professional (CBCP) preferred.	300 hours

protiviti®

High-Level IT Audit Project Scopes (continued)

In addition to the recommended 3-year audit plan outlined above, we have also provided the following reviews for management's consideration.

Additional Potential Projects			
IT Audit	**Recommended Effort**	**Suggested Skill Sets**	**Estimated Hours**
Demand and Portfolio Management	• Detailed review of Demand management process with associated controls and KPIs. • Evaluation of IT project demands and intake processes of technology-related projects both with ICT and Aviation Maintenance. • Assess how demands on IT are classified, prioritized and the oversight in place around the assignment of work to the appropriate resources, and management of the execution of work and validation of service.	• Experience and understanding of best practices around Demand, Program, and Portfolio Management. • ITIL Foundations or Practitioner Certifications preferred • Solid understanding of Project Management and SDLC	250 hours
Vulnerability Management	• Assessment of how vulnerabilities within the Port environment (both internal and external) are identified, risk ranked, addressed and monitored overall. Typically encompasses the patching process.	• Experience with common vulnerability tools (e.g., Nessus, Qualys, etc.) • CISSP	200 hours
Security Strategy Review	• Review of overall security strategy and posture, the approach for strategy development, and how the strategy is being rolled out.	• General knowledge of Security strategy development and implementation • CISSP	200 hours

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:

- ✓ The IT Process Institute's ***IT Controls Performance*** which includes comparison data points on organizational size and IT control effectiveness.
- ✓ The IT Process Institute's ***IT Strategic Alignment Benchmark*** which includes comparison data points on IT strategy models and alignment practices.
- ✓ 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.

This section outlines the results of these benchmark comparisons.

Benchmarking Results

Key Themes

- ✓ 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.
  - The Port may have an opportunity to leverage third-party contractors to help manage costs on some initiatives.
- ✓ Business needs indicate that the primary strategic focus of the Port's IT functions should be on partnering with the business, utilizing a "Process Optimizer" model. The core IT practices to enable this level of alignment are currently in place (per the ITPI Strategic Alignment Benchmark).
  - The need for the "Process Optimizer" alignment model is 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 variations in IT expectations and utilization levels.

Benchmarking Results

Key Themes (continued)

- ✓ The Port's IT processes 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.
- ✓ The Port should consider revisiting these benchmark measurements every 2 – 3 years.

IT Controls Performance Benchmark Results

protiviti®

ITPI IT Controls Performance Benchmark

Overview

- ✓ The ITPI IT Controls Performance (ITCP) Benchmark includes control data from 377 organizations of various sizes and industries between 2007 and 2011.
- ✓ The benchmark measures the maturity of 53 process activities as well as 15 key performance metrics.
- ✓ Analysis of the benchmark results compared the Port's performance across 15 performance metrics to the following industries classifications (identified by the ITPI), each of which has relevant similarities to the Port's business model:
  - ***Energy and Utilities*** – This industry was included based on some utility services provided by the Port. Additionally, the Port can also be viewed as a 'utility' based on the limited number of alternatives within the region.
  - ***Government & Public Administration*** – This industry was included for comparison based on the Port's status as a public commission.
  - ***Transportation*** – This industry includes airport services, marinas, and marine ports & services.
  - ***Professional Services*** – This industry includes real estate operations, commercial building management, IT services, and parking services.
  - ***Miscellaneous Services*** – This industry was added as some Port services do not fit into other industries as defined by the ITPI.

protiviti®

ITPI IT Controls Performance Benchmark

Overview (continued)

- ✓ While the activities of both the ICT and Aviation Maintenance organizations were considered for this benchmarking exercise, the metrics utilized in the final analysis were based solely on ICT data due to the following factors:
  - Discussions indicated differences in metric availability between the two groups.
  - Aviation Maintenance practices showed a lower level of overall maturity and formality when compared to ICT practices.
  - There are on-going efforts to adopt consistent practices across both groups that will utilize ICT's practices as the target / baseline
  - ICT activities represent a significantly greater volume of IT process activity than Aviation Maintenance.

ITPI IT Controls Performance Benchmark

Results Summary

The ITCP Benchmark identified the Port of Seattle as "High Performer" for its peer group.

The "High Performer" designation indicates that the controls that have been implemented have improved the overall performance of ICT, and ultimately the business.

Analysis of the ITCP benchmark results provided the following key observations:

- ✓ The Port's IT performance levels are consistent with those observed across the benchmarking peer group.
- ✓ Potential opportunities exist for additional IT performance gains with targeted IT process improvements.

This analysis and key observations are described in more detail on the following pages.

protiviti®

ITPI IT Controls Performance Benchmark

Industry Analysis

The chart below summarizes the Port's ITCP benchmark analysis for key control use and performance, and it compares the Port's scores to the average scores for "High Performers" in the Port's peer group as well as comparable industry groups.

	Port of Seattle	Peer Group High Performers	Scores (By Industry)				
			Energy and Utilities	Government & Public Admin	Transportation	Professional Services	Misc. Services
Performance "Top Half"	66% (10 of 15)	67% (10 of 15)	50% (7.5 of 15)	52% (7.8 of 15)	33% (5 of 15)	45% (6.7 of 15)	52% (7.8 of 15)
Key Controls in Use	43% (23 of 53)	68% (36 of 53)	58% (30.5 of 53)	59% (31.4 of 53)	57% (30 of 53)	74% (39 of 53)	47% (25 of 53)
Foundational Controls	50% (6 of 12)	69% (8.3 of 12)	55% (6.6 of 12)	60% (7.2 of 12)	51% (6.17 of 12)	71% (8.57 of 12)	62% (7.4 of 12)
# of Firms	N/A	N/A	29	15	6	21	5

Although the Port had fewer key controls considered as "in place" (only 23 of 53) than its peer group or the comparable industry averages, the Port's performance significantly exceeds these industries based on the number of Port performance metrics that are better than half the other respondents (the "Top Half Count").

protiviti®

ITPI IT Controls Performance Benchmark

Metrics Introduction

As mentioned previously, 10 of 15 ICT metrics were higher than at least half of the other participants in the ITPI IT Controls Performance Benchmark. The charts on the next two slides compare the Port's performance metrics to those in the Port's peer group. The average scores are shown as ranges of the 25th to 75th percentile in order to compare the Port's results to middle range of each performer category. Key results and notes related to this analysis are noted below.

Metrics of note:

- ✓ The Port's Server to System Administrator Ratio (the number of servers and other devices that can be supported by a single system administrator – a key IT efficiency measure) greatly exceeds the average. This is attributable to the Port's investment in virtualized servers and efforts to standardize devices and configurations.
- ✓ Although the Port's Percentage of Late Projects is within the range of it's peer group, it does not fall within the top half percentage of all respondents. Discussions indicate that these delays typically result from resource constraints that are typically out of the project teams' control (e.g., key resources not having availability, stakeholder requests to delay the project, business priority changes).
- ✓ Customer Satisfaction results are based on responses from key Port business personnel interviewed for this project. While not in the top half, these scores show the business views ICT in a generally positive light.
- ✓ The Port does not actively track "Emergency" changes. Rather, changes are categorized as Scheduled or Unscheduled. The project team worked with ICT management to review the Unscheduled changes in order to identify changes that appear to meet the criteria of an 'Emergency' change (i.e., addressing network outages, significant application outages).

protiviti®

ITPI IT Controls Performance Benchmark

Performance Metrics Comparison

Performance Measure	Port of Seattle	Peer Group – High Performers
Operations Metrics		
Change Success Rate	***98%***	95 – 98%
Emergency Change Rate *	***7%***	3 – 10%
Late Project Rate *	34%	10 – 50%
Server / System Admin (ratio)	***225.12***	25 – 123
Support Metrics		
First Fix Rate (%)	***95%***	82 – 95%
Incident SLA Rate (%)	***100%***	90 – 98%
Large Outage Mean time to repair (in hours) *	***3***	1 – 4

BOLD GREEN - Performance Metric is better than half of the other respondents in the benchmark

* Lower score is better

** Mean score used rather than median

protiviti®

ITPI IT Controls Performance Benchmark

Performance Metrics Comparison

Performance Measure	Port of Seattle	Peer Group – High Performers
Security and Audit Metrics (based on known security breaches)		
Security Breaches with No Loss (%)	***100%***	99 – 100%
Security Breaches Corrected (%)	***100%***	90 – 100%
Security Breaches Auto Detected (%)	***95%***	80 – 98%
Repeat Audit Findings (%) *	***0%***	0 – 42%
Customer Satisfaction Metrics ** (based on average customer satisfaction survey responses on a 1 -5 Scale)		
End User Satisfaction	3	3.9
Business Management Satisfaction	3	3.6
IT Staff Customer Awareness	4	4.2
IT Staff Customer Communication	3	3.6

BOLD GREEN - Performance Metric is better than half of the other respondents in the benchmark

* Lower score is better

** Mean score used rather than median

protiviti®

ITPI IT Controls Performance Benchmark

Conclusions & Recommendations

- ✓ Continue efforts to align and standardize IT processes across ICT and Aviation Maintenance. These efforts should improve the overall maturity of the Port's IT processes and simplify the management of key IT systems.
- ✓ The ITPI research suggests that the Port's overall IT performance can realize additional gains by continuing to mature three building block process activities:
  - A defined process to detect unauthorized access;
  - Defined consequences for intentional, unauthorized changes; and
  - A defined process for managing known errors (currently in place).
- ✓ After improving the controls listed above, the Port should explore maturing the additional nine foundational process activities, which will continue to improve performance objectives (see Appendix B for a listing of the foundational activities).

protiviti®

ITPI IT Controls Performance Benchmark

Conclusions & Recommendations

- ✓ The Port should consider revising the Change Management Meeting structure to define specific guidelines governing what can be considered as an "Unscheduled Change."
- ✓ The Port should evaluate whether the business has a desire to implement a process to define, report, and measure IT service level objectives.
  - This will help ensure the business understands the desired / requested levels of IT service as well as the IT function's ability to delivery against these objectives.
  - Defined service level objectives will also enable better planning within the IT organization related to meet business expectations.

protiviti®

IT Strategic Alignment Benchmark Results

protiviti®

ITPI IT Strategic Alignment Benchmark

Overview

Protiviti utilized the IT Process Institute's IT Strategic Alignment (ITSA) Benchmark study to better understand how the Port's IT function aligns with the overall business strategy. Based on this research, IT organizations fit one of three types when considering IT and Business Alignment:

IT Organizational Types	
Utility Provider	Not always engaged with the business. Focused primarily on providing shared information management services and support needs.
Process Optimizer	Responsive to the business. Focused on shared information management services and support, plus improving business applications and business processes.
Revenue Enabler	Well integrated into the business. Focused on shared information management services, business process optimization, and technology enabling products and services.

The dominant organizational type helps to define and clarify IT's focus and its impact on the overall business strategy.

- ✓ When an IT organization focuses on adding business value without confirming the type fit, it risks becoming fragmented as it attempts to move in multiple, counterproductive directions.
- ✓ Business executives may not clearly articulate the business strategy, IT management may not be actively integrated into the business, or a combination of the two may exist.

ITPI IT Strategic Alignment Benchmark

Overview (continued)

- ✓ The ITPI ITSA Benchmark includes control data from 269 North American companies across various industries.
- ✓ This data analyzes nine value attributes, 49 alignment practices, and16 alignment measures to determine the specific practices that enable IT strategic alignment success.
- ✓ This analysis utilized two methods to gather information necessary to conduct this assessment:
  - Key business personnel were polled (via inquiry and questionnaire) on nine questions used to determine the 'type' of IT organization needed to achieve the level of value desired by the business.
  - Facilitated sessions were conducted with the ICT and Aviation Maintenance leadership to gather 89 data points related to alignment practices and measures.
- ✓ After gathering the necessary information, the project team compared the business' expected type of IT to how the IT function has structured itself.
- ✓ Additionally, the project team was able to determine if the Port has implemented the specific strategic alignment practices that have been found to optimize alignment for the desired IT type.

protiviti®

ITPI IT Strategic Alignment Benchmark

Nine Organizational Attributes

The type of IT Organization identified by the benchmark is determined by specific organizational attributes based on the IT function's focus on the following set of Information Management, Business Process, and Strategic Revenue activities.

Attribute	Information Management	Business Process	Strategic Revenue
1. Purpose	Provides shared services—common infrastructure and information management	Enables business unit objectives, and focuses on application and process improvement to differentiate customer offerings	Enables technology-based products and services to enter new markets
2. New technology requirements	Improve cost and efficiency	Meet specific business function requirements	Enable new product or service
3. CIO role	Operations expert	Business manager	Corporate strategist
4. CIO reports to	Finance or Operations	Business unit executive	CEO / President
5. IT funding source	Independent as shared service	Part of business unit budget cycle	Part of enterprise strategic planning
6. Success metrics	Operating performance SLAs and user satisfaction	Project success and business unit executive satisfaction	Enterprise-level revenue contribution
7. Business strategy participation	IT is not involved in determining business goals and strategy	IT collaborates at the business-unit level	IT plays a proactive role in shaping corporate strategy
8. Competitive advantage contribution	Cutting costs, reducing inefficiencies, and enabling better decision making	Optimizing business functions and business processes to differentiate existing products and services	Creating new technology-enabled products and services that change the rules of the game
9. Investment justification	Cost savings and business process efficiency gain	Revenue or profit gains from existing products and services	Revenue and profit that are generated by new products or new markets

protiviti®

ITPI IT Strategic Alignment Benchmark

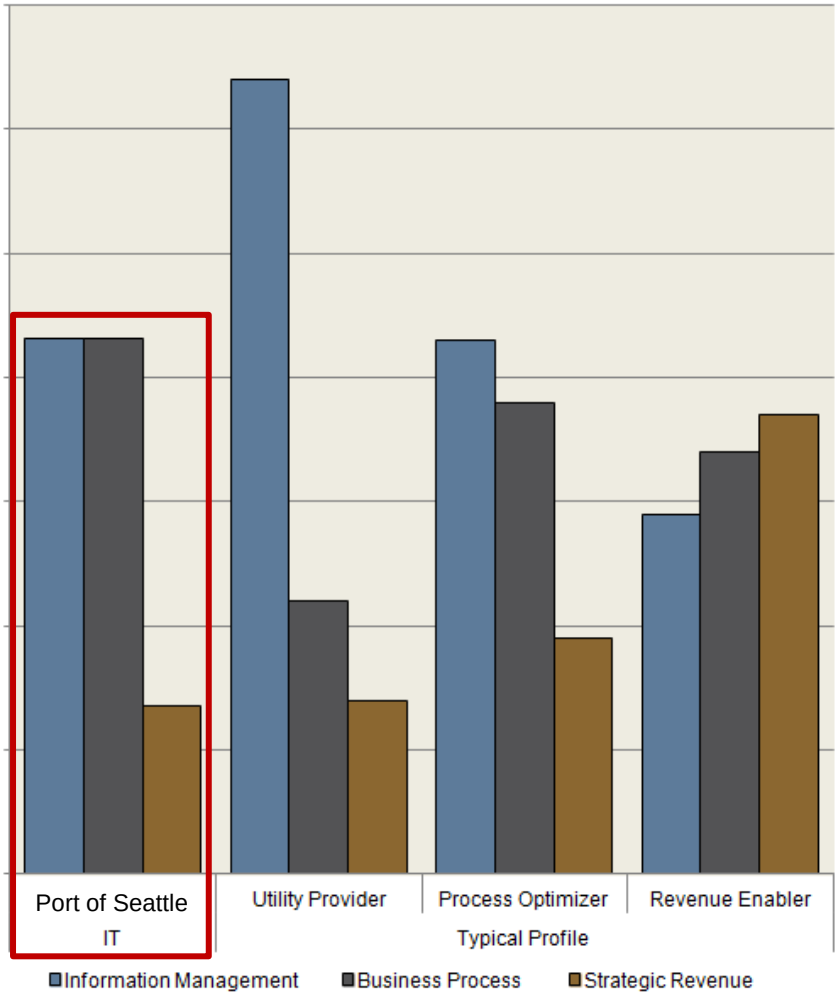
The Business Perspective

- ✓ Surveys were sent to leaders within the various business units in order to profile their desired type of IT function.
- ✓ Based on discussion with key business personnel, profiles of the type of IT function desired by the business were identified. These results indicate the type of IT function desired is dependent on the division of the Port in question:
  - The Seaport, Real Estate, Police / Fire, and Capital Development divisions desire an IT function that focuses on providing consistent, reliable connectivity to the applications they use to perform their jobs. This best aligns with a ***Utility Provider*** IT function.
  - Corporate and the Aviation divisions desire an IT function that can provide innovative solutions that improve their ability to deliver service to their customers. These needs best align with a ***Process Optimizer*** IT function.
- ✓ It is important to note that the majority of IT services (and costs) are currently associated with delivering services to Corporate and the Aviation division. This suggests that the Port's IT function should focus on providing services expected of a Process Optimizer.

protiviti®

ITPI IT Strategic Alignment Benchmark

The IT Perspective



The results of the facilitated benchmark sessions indicate, we determined that the Port's IT function is most accurately described as a ***Process Optimizer***.

- ✓ The chart to the left depicts an aggregate view of the ICT and Aviation Maintenance results weighted by the number of personnel.
- ✓ Aviation Maintenance personnel tend to function as a Utility Provider which is consistent with their current mandate from the business.
- ✓ The benchmark also suggests that in some situations, ICT's activities can lean towards those typical of a *Revenue Enabler*.
- ✓ IT's status as a Process Optimizer appears to be aligned with business expectations because the majority of IT services are targeted to Aviation and Corporate
- ✓ The other divisions that desire a Utility Provider may perceive the processes implemented to support the needs of a Process Optimizer to be excessive and unnecessary. As a result, it is important that cost of these additional services be clearly understood and allocated to the appropriate divisions.

protiviti®

ITPI IT Strategic Alignment Benchmark

The IT Perspective – Process Optimizer Profile

As a ***Process Optimizer***, the Port's IT functions should be focused on providing a common infrastructure and capabilities that support basic information and transaction management. Additionally, the IT function should enable business unit specific objectives and capabilities by implementing applications that optimize key business functions and processes.

Below are the key attributes and drivers of IT functions acting as a Process Optimizer:

- ✓ ***Key Enabler:*** Business is involved with IT planning and strategy
- ✓ ***Key Challenge:*** Balance standardization with unique business requirements.
- ✓ ***Key Measures:***
  - Business unit executive satisfaction
  - Business process efficiency and effectiveness
- ✓ ***Key Performance Drivers:***
  - Actively identifies opportunities to use emerging technology
  - Develops and enforces enterprise infrastructure standards
  - IT investments are justified primarily by business process optimization that enables competitive advantage.
  - Understanding business needs is pervasive at the IT executive and VP level.

ITPI IT Strategic Alignment Benchmark

Conclusions and Recommendations

- ✓ The Port's IT function is appropriately structured as a Process Optimizer to support the objectives of its primary stakeholders within Corporate and the Aviation division.
- ✓ While the other divisions do not desire more than a Utility Provider, the services they receive from a Process Optimizer should be sufficient to meet this need.
- ✓ Port Management should formally select and communicate support for a single IT alignment model to all business units. The Process Optimizer model is likely the most appropriate fit to ensure the same level of service for the Corporate and Aviation divisions.
- ✓ IT functions should be cautious of focusing on alignment practices that overreach the mandate of a Process Optimizer since this could lead to unnecessary additional alignment-oriented activities (and costs).
- ✓ The formula for reallocating IT costs from the Corporate division to the other divisions is viewed as a pain point by "lighter" IT-using divisions. The formula should be reviewed by Management and either reinforced or revised (e.g., to align more closely with the initial IT cost allocation, pre-reallocation, which is based on system utilization).

protiviti®

Gartner Benchmark Matrix Analysis

protiviti®

Gartner Benchmarking Results

Approach Overview

Protiviti utilized the ***Gartner IT Key Metrics Data 2012: IT Spending and Staffing Report*** to compare the Port to other organizations in a variety of similar industries as well as the average for all participants in North America. The following slides show the industry and Port metrics for several key performance indicators. For the purposes of this analysis, the Port was compared to the following industries, each of which has relevant similarities to the Port's business model:

- ✓ ***Government - State / Local*** – This industry was included for comparison based on the Port's status as a public commission.
- ✓ ***Professional Services*** – This industry includes real estate operations, commercial building management, it services, and parking services.
- ✓ ***Software Publishing & Internet Services*** – This industry was included as the Port internally develops customized applications and provides these to some tenants and airlines.
- ✓ ***Transportation*** – This industry includes airport services, marinas, and marine ports & services.
- ✓ ***Utilities*** – This industry was included based on some utility services provided by the Port. Additionally, the Port can also be viewed as a 'utility' based on the limited number of alternatives within the region.

Gartner Benchmarking Results

Assumptions

***Gartner Definitions*:**

- ✓ ***IT Spend*** comes from anywhere in the enterprise that incurs IT costs and it is not limited to the IT organization. It is calculated on an annualized "cash out" basis and therefore contains capital spending and operational expenses, but not depreciation or amortization.
- ✓ ***Number of IT Full-Time Equivalents (FTE)*** represents the logical staff to support functions performed by the physical staff, measured in calendar time. This includes all staffing levels within the organization from managers and project leaders to daily operations personnel. This includes both in-sourced FTEs and Contract FTEs. This excludes staff of a third-party vendor (e.g., IT outsourcing), who are not operationally managed by in-house staff, but managed by the vendor.
- ✓ ***Number of Employees*** is the count of employees (i.e., head count, excluding enterprise contractors and consultants) regardless of whether these employees are frequent users of the technology supported by the IS organization. This includes full-time and part-time employees or as reported in public record.
- ✓ ***Operational Spend*** is the total day-to-day operations and maintenance expenses for this fiscal year that have not been capitalized. This does not include any amortization and depreciation expenses.
- ✓ ***Capital Spend*** includes the total capitalized IT spend for the fiscal year. (Full value of capitalized assets acquired in the fiscal year.) This includes investments in new application development and IT infrastructure.

(Detailed source data used in this analysis is available in the Appendix)

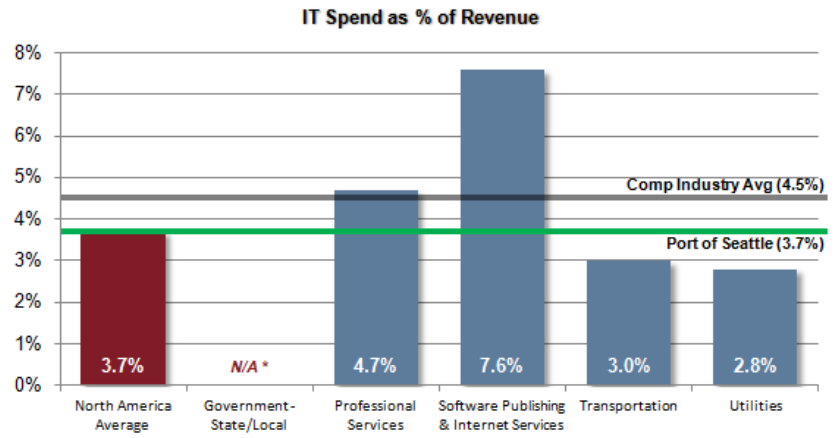
protiviti®

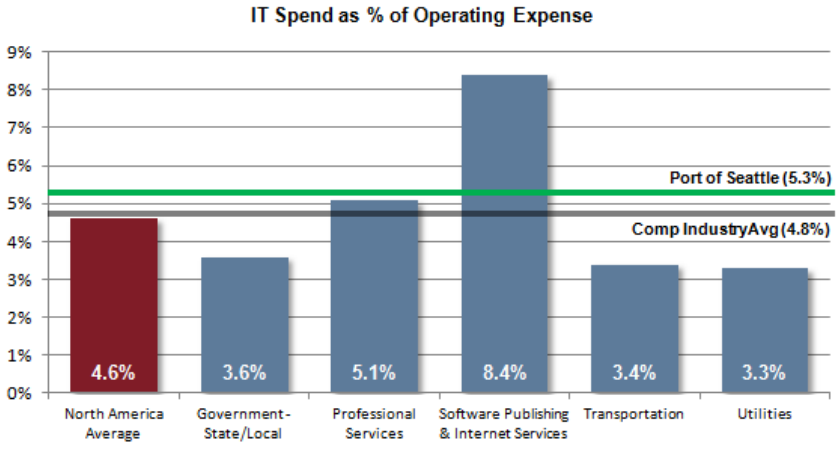
Gartner Benchmarking Results

IT Spend as % of Revenue / Operating Expense

These metrics compare the Port's IT Spending to the Port's Revenue and Operating Expenses. These metrics must be considered in conjunction with other metrics, overall business objectives, and other circumstances that could influence the resulting calculations.

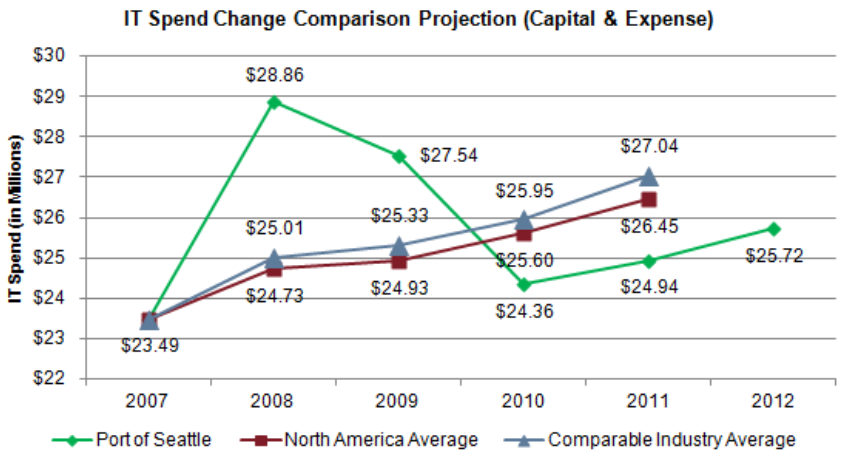
- ✓ ***% of Port Revenue*** – This metric can assist in evaluating whether the level of investment in IT is aligned with business performance.
  - The Port's IT spend is consistent with the average across comparable industries.
  - NOTE: This metric is not calculated for Government entities. As a result, the Comparable Industry Average also excludes this data point.
- ✓ ***% of Port Operating Expenses*** – This metric can also provide a perspective on the business' IT investment strategy based on operating expenses which tend to be more consistent year-to-year.
  - The Port's metric is less than 1% higher than the comparable industry average.
  - This metric is likely influenced by how the Port chooses to capitalize some projects.
  - Additionally, organizations with higher IT spend percentages tend to view IT as an enabler which can improve business performance and productivity. This is consistent with the view of IT as a Process Optimizer.

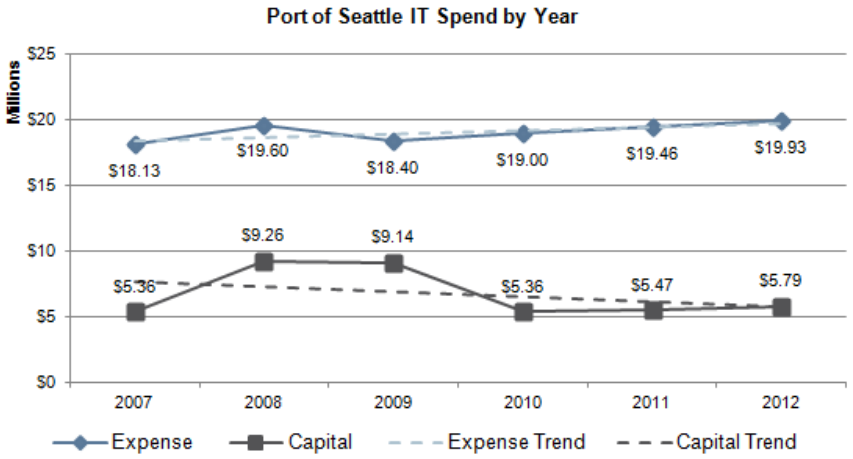




Gartner Benchmarking Results

IT Spending Change Over Time





The charts to the left illustrate how the Port's IT spending has changed from 2007 to 2012. Since the Port's IT spending was generally aligned with comparable industries (see previous slide), Protiviti used the Port's 2007 IT spend as a baseline to project what the Port's IT budget would look like assuming it followed Gartner's average rate of change for North America and comparable industries over the 2007 to 2011.

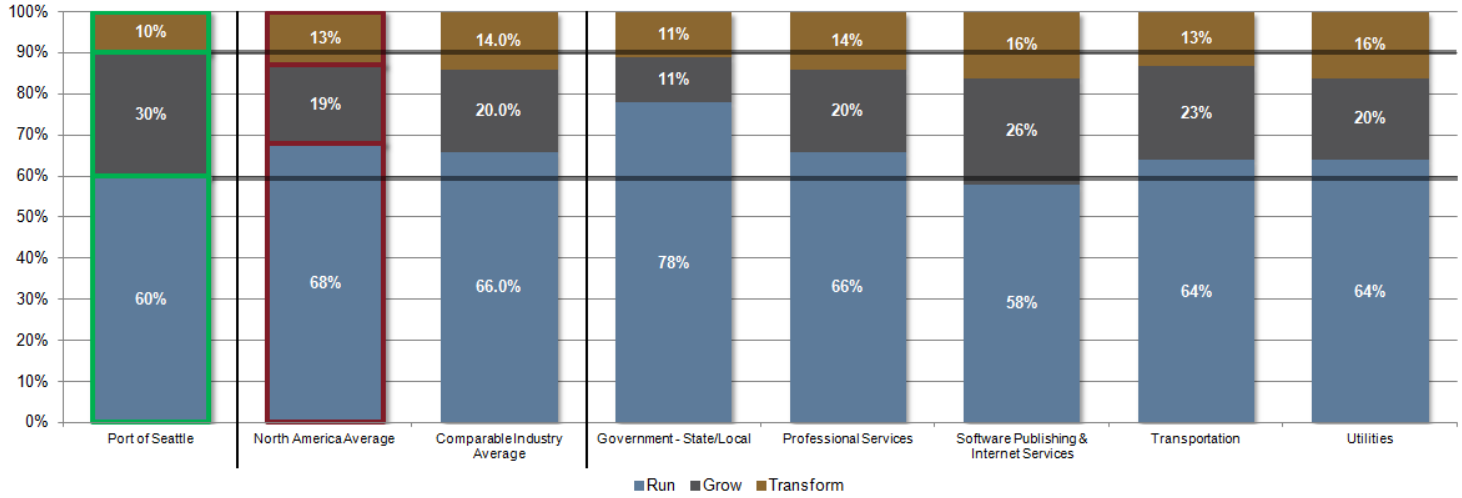
This comparison yielded the following key observations:

- ✓ The Port has demonstrated better IT cost control over the 2007-2011 period (net increase of 9%) than predicted by either the Gartner North America or comparable industry averages (net increases of 13% and 15%, respectively).
- ✓ The Port's cost containment results were achieved despite increased capital expenditures in 2008 and 2009 (~70% higher than either 2007 or 2010). These increases were due to several large capital projects, including HCM Upgrade, IP Telephony, and Computer Aided Dispatch (911 system).
- ✓ While significant capital IT projects (like the 2008 and 2009 examples above) are often accompanied by a subsequent increase in IT expense, the Port's IT expenditures have demonstrated effective cost control over the 2007 to 2011 period, as demonstrated by the following results:
  - Expense increased by only 7% (net) over the period.
  - The Port's cumulative IT expenditures for the period were within 2% and 3% of the amount predicted by the Gartner comparable industry and North America averages.

protiviti®

Gartner Benchmarking Results

IT Spending Supporting Growth and Transformation



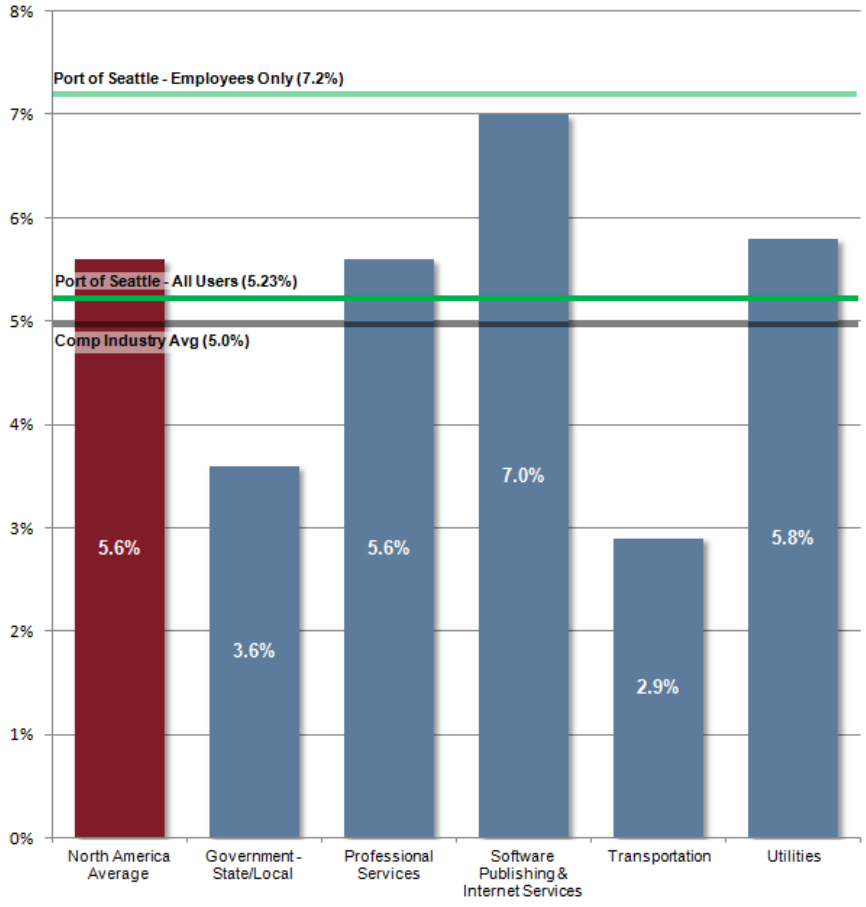
This metric looks at how IT's investments are spread between maintaining the existing IT environment and infrastructure (Run); developing and enhancing technology to support business growth (Grow); and implementing technology to introduce the Port to new business opportunities (Transform). The Port has generally outperformed comparable industries in controlling its "run" costs and has shifted more of its IT spend on growing and transforming the business. This is likely attributable to:

- ✓ Cost reductions in supporting the IT infrastructure (i.e., server virtualization, device standardization)
- ✓ Viewing the IT function as an enabler of business objectives also impacts these allocations as the IT function prioritizes investments in projects that will grow or transform business operations.

protiviti®

Gartner Benchmarking Results

IT FTEs as a % of Employees



This metric compares the ratio of IT FTEs to the number of employees / users they support. This ratio helps to determine whether the IT function's staffing is aligned with business needs.

- ✓ On initial analysis, the number of employees supported by Port IT personnel appears to be high (7.2%). However, Port IT personnel support end users who are not Port Employees (i.e., contractors, tenants, airline users). Adjusting the metric to account for these additional users better aligns the Port's ratio (5.2%) with the average results.
- ✓ The percentage of IT FTEs across related industries varies, however the average percentage across related industries is 5% which is slightly lower than the Port's average of 5.2%.
- ✓ The Port's ratio may be attributed to the Port IT function acting as a "Process Optimizer" which typically employs additional resources that specialize in addressing specific business needs. This is similar to the Professional Services and Software Publishing & Internet Services industries.

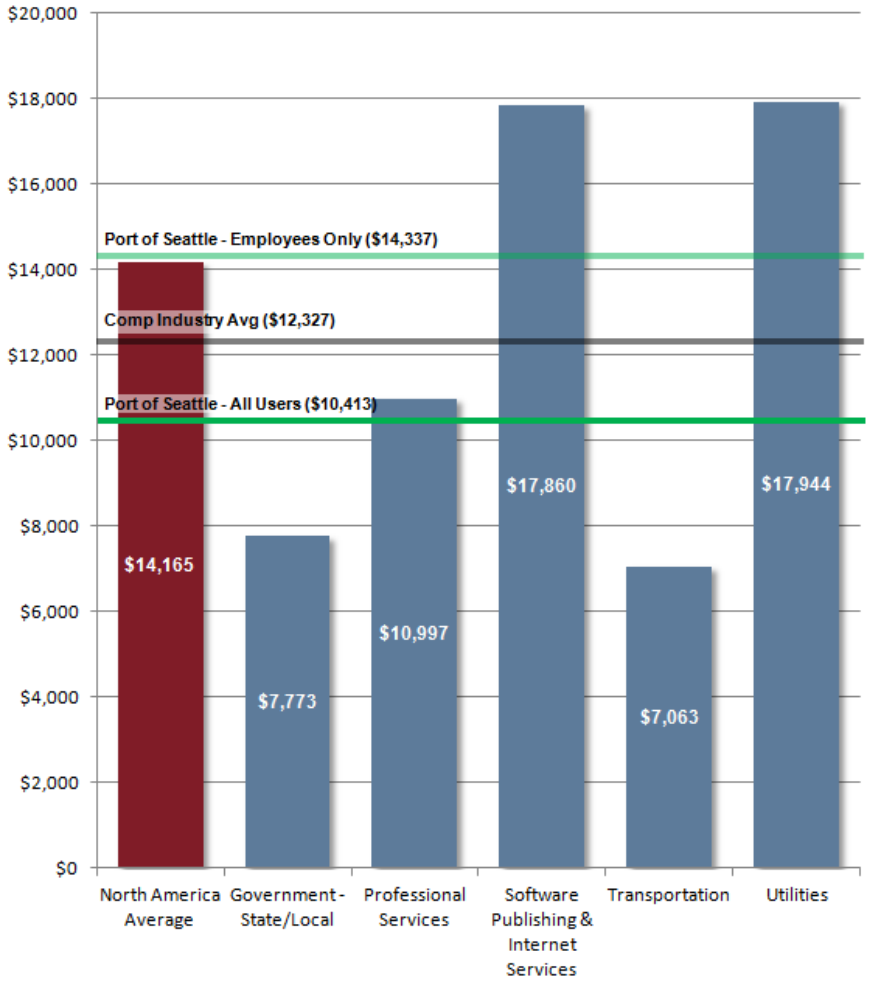
protiviti®

Gartner Benchmarking Results

IT Spend Per Employee

This metric looks at the average IT spend per Port employee. This provides an indicator of the level of IT support received by the end users.

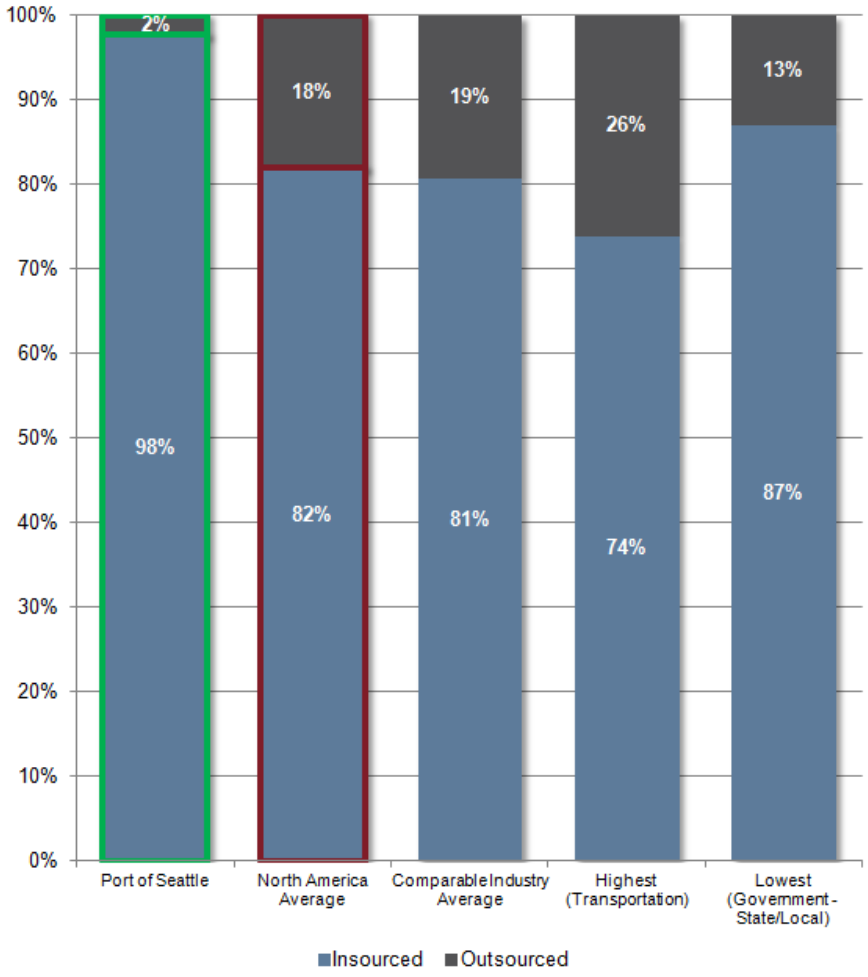
- ✓ The initial analysis shows the Port's IT Spend per employee is ~$2,000 higher than the comparable industry average although lower than some comparable industries. However, like the IT FTEs as a % of Employees metric, this does not account for non-employees supported by the IT functions.
- ✓ Adjusting the metric to account for the additional non-employees brings the average IT spend below the comparable industry average.
- ✓ The actual value of this metric should be viewed as between the employee only and all user values as the same level of service is not required between Port and non-Port employees.
- ✓ It should not be considered unusual for the Port to have a higher than average IT spend per employee given the number and diversity of systems supported by the IT functions.



protiviti®

Gartner Benchmarking Results

Use of Contractors



This metric compares the use of internal versus external resources in delivering IT services. Contractors enable the organization to remain flexible to changing business conditions. However, reliance on contractors for extended periods can be costly and may adversely affect efforts to implement a standardized approach.

- ✓ The majority of IT services at the Port are provided by internal ICT or ET resources.
- ✓ This reliance on internal resources is an outlier in comparison to other industries.
- ✓ Recent changes to Port procurement requirements and limitations on the time period contractors can be engaged for.
- ✓ Additionally, the use of contractors may be prohibitive based on the complexity and diversity of the Port's operations which require additional time to onboard contract resources.

protiviti®

Gartner Benchmarking Results

Conclusions & Recommendations

- ✓ Due to the Port's complex environment and diverse service, it is important to consider the Port's metrics in comparison to several different comparable industries.
- ✓ The Port's IT metrics are generally aligned with the comparable industry averages.
- ✓ With the exception of the use of contractors, higher than average Port metrics are not significant outliers and can be attributed to several causes:
  - IT functions acting as a Process Optimizer typically have higher costs and resource needs than comparable industries to support the organization's. With the exception of Professional Services and Software Publishing / Internet Services, most IT organizations in comparable industries tend to act as utility providers.
  - The Port has needed to develop applications to address business objectives because out-of-the-box solutions do not exists to support these objectives.
  - The number and diversity of application within the application portfolio require additional resources and expenses to support.
  - Port IT functions support end-users who are not Port employees.
- ✓ Industry benchmarking should be revisited every 2-3 years to revalidate and re-baseline IT performance.

protiviti®

Gartner Benchmarking Results

Conclusions & Recommendations

- ✓ An opportunity may exist to better leverage contractors to assist in delivering IT services to the business and contain IT costs. However, to realize this opportunity, the following sourcing challenges should be addressed (in collaboration between IT and Procurement):
  - Streamline the process of engaging contractors to assist on critical IT projects to allow for "just-in-time" staffing of contractors.
  - Review the policy limiting contract resources to a single year of service. The ramp-up time required for new contractors limits their effectiveness, and could potentially increase IT costs due to this policy.
- ✓ Continue efforts to streamline the application portfolio by consolidating applications with similar functionality and encouraging the use of existing applications rather than implementation of new applications.
- ✓ Business leaders need to identify specific metrics that should be reported by IT to stakeholders (e.g., the ICT Governance Board).
  - Metrics should be shared regularly with key IT stakeholders and trended over time.
  - A subset of key metrics should be identified for regular communication to the Port Commission.

Technology Performance: Process Maturity Analysis

protiviti®

Capability Maturity Analysis

Approach Overview

- ✓ Over the course of the assessment, the Protiviti project team conducted interviews with ICT and Aviation Maintenance personnel in order to gain a better understanding of how key IT processes were performed across the Port. The specific processes reviewed were:
  - Change, Configuration & Release Management (includes SDLC)
  - Continuity Management
  - Program, Project & Portfolio Management
  - Security Management
  - Support / Service Desk
- ✓ The maturity of each of these processes across all Port IT functions was evaluated using the Capability Maturity Model and the Six Elements of Infrastructure.
- ✓ The Project team also evaluated the maturity of the Port's IT Governance practices across the Five Elements of IT Governance as defined by the IT Governance Institute.
- ✓ Additional information about the Capability Maturity Model, Six Elements of Infrastructure and Five Elements of IT Governance can be found on the following pages.

protiviti®

Capability Maturity Analysis

Results Summary

- ✓ The Port's IT functions have established a core set of IT process, human, and technological capabilities to enable consistent delivery of IT services.
- ✓ Based on the Port's desire to balance cost control with IT performance, this analysis identified a "Defined" level of maturity as an appropriate target for the Port.
  - Areas currently meeting or exceeding the Port's maturity requirements include: Project, Program & Portfolio Management and IT Support & Service Desk.
  - Areas largely aligned with the Port's maturity requirements but with some additional opportunities for improvement include Change, Configuration & Release Management and IT Governance.
  - Areas where additional improvement is required to align with the Port's maturity requirements include Continuity Management and IT Security.
- ✓ Further maturity improvements can be expected as the effort to align and standardize ICT and Aviation Maintenance IT processes are completed.

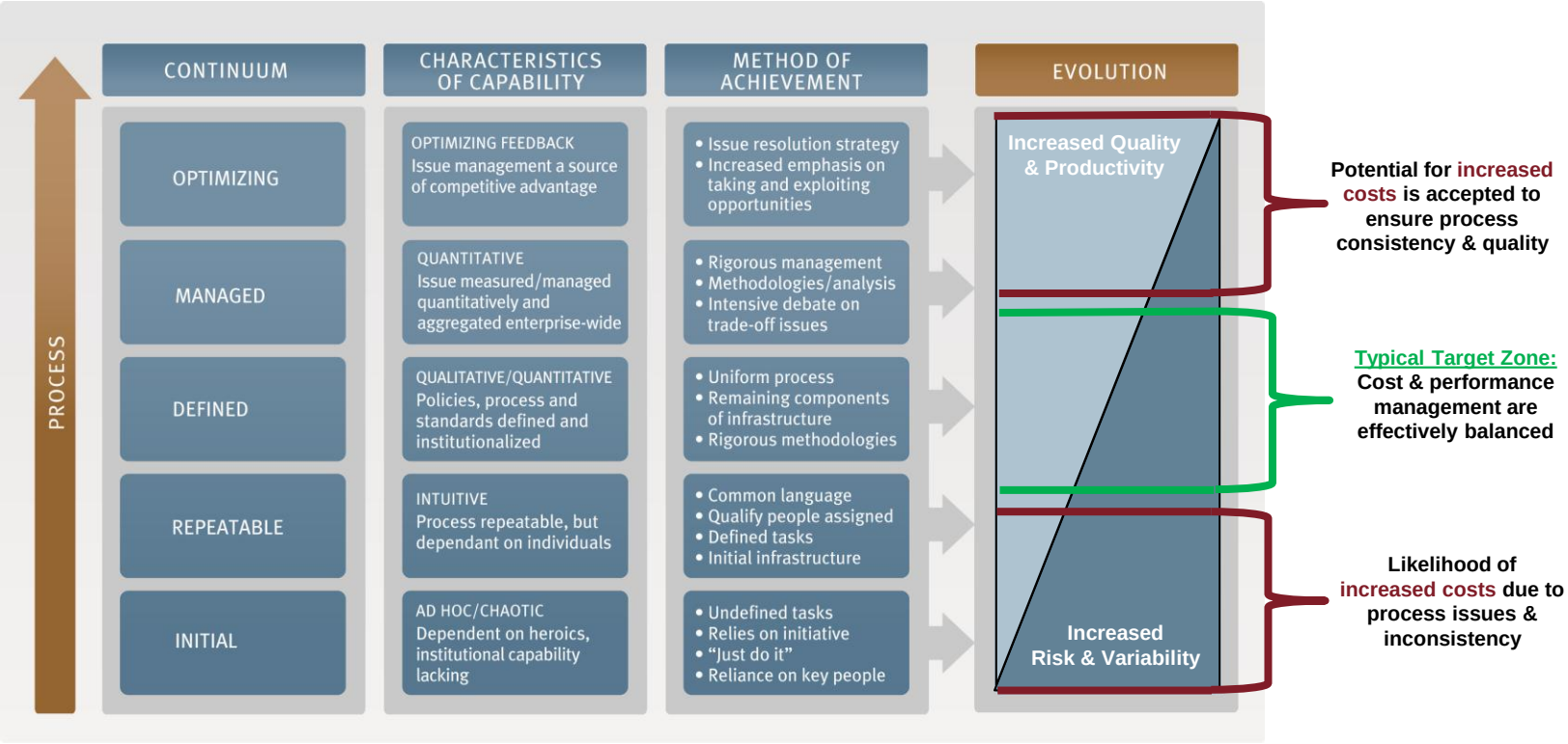
The results and recommendations from this analysis are described on the following pages.

protiviti®

Capability Maturity Analysis

About the Capability Maturity Model

The Protiviti Capability Maturity Model is a methodology, adapted from the SEI Carnegie-Mellon Capability Maturity Model, used to develop and refine an organization's processes. The model describes a five-level evolutionary path of increasingly organized and systematically more mature processes. The model is depicted in the graphic below:

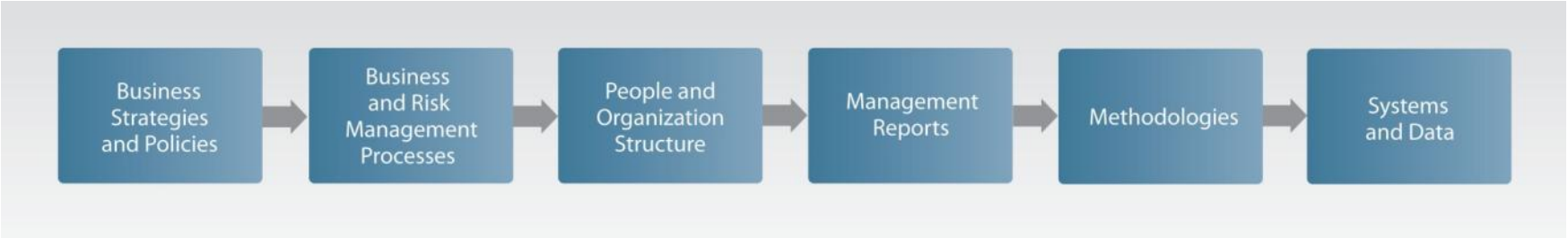


protiviti®

Capability Maturity Analysis

About the Six Elements of Infrastructure

The Six Elements of Infrastructure (Six Elements) is a tool for categorizing issues, understanding where problems are occurring within the organization, and drawing conclusions to form the basis for recommendations. These capabilities should be a part of every process and function should possess. The Six Elements are identified in the graphic below:



The Six Elements are used in conjunction with the CMM to determine the needed improvements in process capability. The following slides outlined specific observations associated with each element of the Six Elements. More detailed explanations of each element are described in the Appendix.

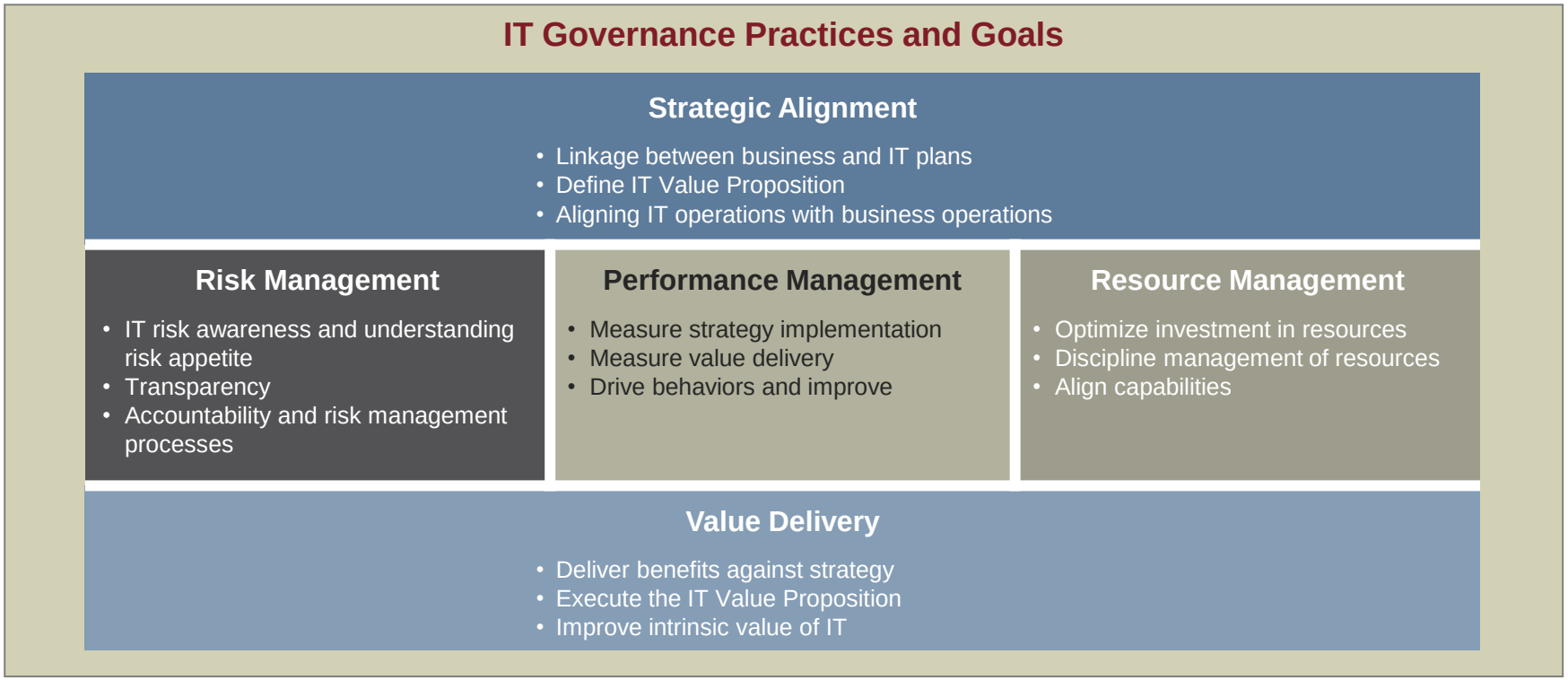
(IT Governance is evaluated by the key areas of IT governance rather than the Six Elements of Infrastructure)

protiviti®

Capability Maturity Analysis

About the Five Elements of IT Governance

When assessing the Port's IT Governance activity, the project team used the IT Governance Institute's The Five Elements of IT Governance (depicted below) instead of the Six Elements of infrastructure to identify the specific governance practices and provide a basis for the maturity assessment.



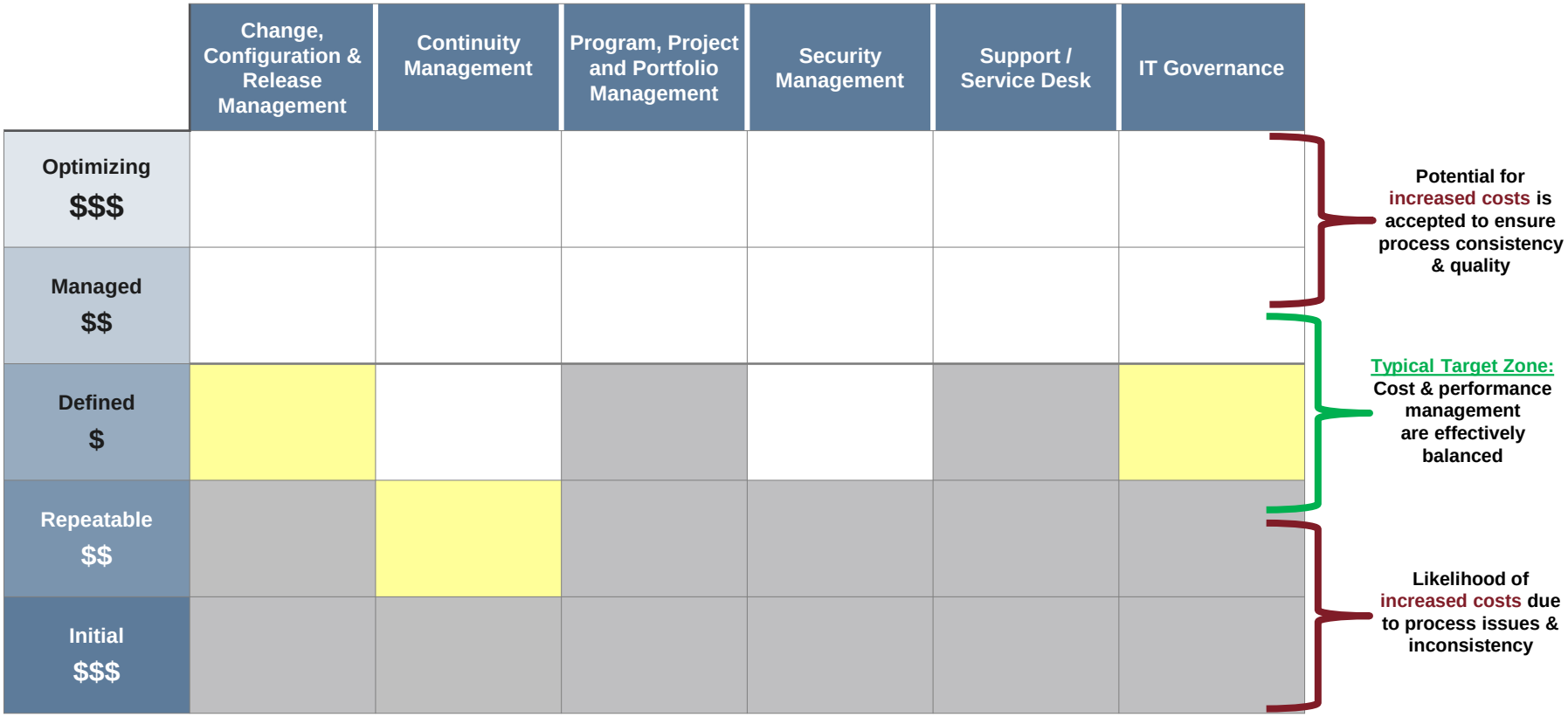
protiviti®

Capability Maturity Analysis

IT Capability Maturity Analysis Summary

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

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



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

Capability Maturity Analysis

IT Operational Processes (1 of 2)

Change, Configuration & Release Management	● IT has implemented the AGILE development methodology to facilitate the development process for custom-developed applications. ● Development teams utilize Microsoft's Team Foundations Server (TFS) to manage the development process, including requirements for robust development documentation. ● IT holds a weekly change management meeting to discuss changes that will occur over the upcoming week. However, there is little discussion of the impact of each change during the meeting. ● A larger than average number of changes are considered "unscheduled" (made outside of the change management meeting cycle) than similar organizations. These changes are not necessarily to address a system outage or other situation. ● IT is in the process of implementing the Tripwire application for file integrity monitoring; however IT is currently unable to automatically detect unauthorized production environment changes. ● IT utilizes customized SharePoint ticketing functionality to manage changes and a custom-developed configuration management database (CMDB) tool; however, these data sources are not integrated and the CMDB data is not consistently updated to reflect changes. They are also not integrated with the Service Desk system (Maximo) or TFS.
Continuity Management	● IT has deployed technology that is designed to be resilient and would likely experience minimal downtime during a business interruption. ● The existing BCM policy has not been updated since 2006 - efforts to update are underway. ● Existing data centers provide limited geographic diversity - efforts to establish an additional site are in-process. ● BCM and IT recovery plans have not been fully tested. ● It does not appear that a Business Impact Analysis has been performed with the business to establish recovery time and point objectives to appropriately scope IT recovery operations. ● Although Continuing Operations Plans are being consistently developed across the business, there is not a centralized analysis by IT to ensure that recovery plans appropriately consider system downtime.

● Defined (On Target) ● Repeatable (Improving) ● Initial

protiviti®

Capability Maturity Analysis

IT Operational Processes (2 of 2)

Project, Program & Portfolio Management	● Significant efforts have been made to implement a consistent project management approach within IT. ● Project Managers and Business Analysts (BAs) have obtained PMP and BA certifications. ● ICT Governance Board meets at least once a month to report on the progress of the project. ● IT projects typically are delivered within budget, and 66% of IT projects are delivered on time. ● In the past, IT has been brought into some business initiated projects after the scope and cost have been established. Efforts have been undertaken to improve integration and communication between IT and Business project management efforts. ● Projects delivered outside of defined timeline expectations are often the result of changed business project sponsors priorities or key business resources availability.
Security Management	● The Port has recently hired a Senior Manager, CISO with responsibility for the Port's overall security posture. ● The Port has undertaken efforts to assess their PCI compliance but remediation activities have not be completed consistently. ● A comprehensive Information Security policy has not been published. ● Processes have not been implemented to regularly review user access to IT systems. ● Individuals requesting access to IT systems generally do not know the specific type of access needed.
Support / Service Desk	● A centralized Service Desk has been implemented to handle all in-coming requests. ● Maximo is utilized by IT to manage, track, and report on incidents and service requests. ● ICT provides internal users access to a growing knowledge base for user self service. ● Incidents are tracked and prioritized by severity level. Data show that these issues are typically resolved within internal service level goals. ● IT personnel focus on addressing incidents. There is minimal focus on incident trending or correlation in order to identify underlying problems, and known error tracking is informal.

● Defined (On Target) ● Repeatable (Improving) ● Initial

protiviti®

Capability Maturity Analysis

IT Governance Practices

Strategy Alignment	● Clear Governance Board approval requirements have been established for investments exceeding specific thresholds. ● Governance board is comprised of business and IT executives ● Based on the results of the ITPI Benchmarks, it appears that the IT functions are appropriately aligned with business expectations.
Risk Management	● IT has conducted a risk assessment and is actively tracking / addressing the identified items on a dashboard. Progress is communicated intermittently in the ICT Governance Board meetings. ● Ongoing project risks and issues are communicated up to management through formal channels. ● Key IT risk and key controls have been identified for the Port's financial systems, but these are not necessarily reviewed and verified for all IT systems.
Resource Management	● Turnover is low and few contractors are utilized within IT which enables the staff to better understand key resource capabilities. ● Skills have been identified for each IT role, and managers regularly review/assess needs. ● The inventory of skill sets is effectively managed by individual IT managers.
Performance Measurement	● IT has mechanisms in place to gather the information necessary to measure their performance. ● Information is provided to the executive leadership, but not necessarily at their request. ● IT has not worked with the business to define service level expectations making it difficult for IT to demonstrate that service objectives are being met.
Value Delivery	● From a PMO standpoint, there are activities in place to confirm capital project requirements are being met, budget is kept, and goals are being achieved. ● While the concept of "ROI" is not regularly used, post-project reviews validate that goals established in business cases are met by completed projects.

● Defined (On Target) ● Repeatable (Improving) ● Initial

protiviti®

Capability Maturity Analysis

Recommendations (1)

Change, Configuration, & Release Management:

- ✓ Incorporate risk-based impact assessment into the change management meeting and change review process. This process should leverage data from the Port's CMDB as well as individuals' knowledge. Key outcomes from this process should include:
  - Designation of different levels of review, approval, and validation required for a change.
  - Increased flexibility in change scheduling and a reduction in "unscheduled" changes (e.g., lower impact / risk changes could be approved with less lead time).
- ✓ Formally incorporate configuration data updates (via the CMDB) into the change management process to help ensure configuration data reliability. These efforts should also include a review of the CMDB data structure to ensure it supports all the needs of the change and support management processes.
- ✓ *(Beyond Target Goal)* - Complete implementation of the Tripwire file integrity monitoring solution and institute a formal process for reviewing and resolving detected changes. This process should also include defined consequences for implementation of changes without proper approval.
- ✓ *(Beyond Target Goal)* - Evaluate whether the Maximo application functionality can be extended to support the change management process to enable better alignment between the support and change management processes, and also streamline performance reporting / monitoring for IT processes. These efforts should also consider whether the CMDB data can be integrated with Maximo.

protiviti®

Capability Maturity Analysis

Recommendations (2)

Continuity Management:

- ✓ Define a clear schedule for updating the Port's overall BCM policy, aligning Continuing Operations Plans, and creating a cross-department IT continuity plan.
- ✓ Perform a comprehensive business impact analysis (BIA) spanning all Port divisions to establish clear business recovery objectives (RTO and RPO).
- ✓ Continue with in-process plans to establish a recovery site in a different geography than the Puget Sound Region (e.g., Spokane).
- ✓ Perform tests across IT and the business to validate effectiveness of the updated BCP, Continuing Operations Plans, and IT recovery procedures. This could begin with less complex / detailed procedures (e.g., a desktop walkthrough) but should progressively build up to a full end-to-end recovery test for business critical business functions and applications.

Project, Program, & Portfolio Management:

- ✓ *(Beyond Target Goal)* - Continue efforts to align IT and capital project management across the enterprise. As part of these efforts, there should be a formal process for IT architectural / impact assessment at the outset of all capital projects with anticipated IT impacts. This should verify alignment with existing IT architectural standards, consider impacts to compliance frameworks, and evaluate whether other IT risks are effectively mitigated.

protiviti®

Capability Maturity Analysis

Recommendations (3)

Security Management:

- ✓ Continue efforts to remediate PCI compliance gaps. As part of these efforts, management should evaluate the resource requirements for the Security organization and develop formal resourcing plans to align with the compliance project objectives.
- ✓ Develop and distribute a comprehensive IT security policy. These efforts should be paired with a formal security awareness program for all Port employees and system users.
- ✓ Define and implement formal user access review processes. These processes should involve validation of user access permissions with the appropriate system owners (where possible, the system owners should be business unit personnel).
- ✓ Formalize the roles / permission sets granted to users for key systems based on job function.
    - These roles / permission sets should be utilized to determine appropriate approvals for granting new or additional access to Port systems.
    - Key incompatible roles / permission sets should be identified (with the business, where applicable) and these should be evaluated at the time of access provision as well as on a recurring basis to verify proper segregation of duties.

Capability Maturity Analysis

Recommendations (4)

Support / Service Desk:

- ✓ Define a formal process for identifying and managing problems, including creation of a centralized repository of "known errors" and workarounds (as part of the Port's support knowledge base).
- ✓ *(Beyond Target Goal)* - Review the design and operation of the existing Maximo service desk solution to identify points of sub-optimization and opportunities to streamline the application for IT and business users. In addition to the design of the Maximo service desk workflows, these efforts should also consider the following:
  - Ease of data entry / collection and opportunities for increased user "self-service" (e.g., providing a sub-set of IT services in a standard "catalog").
  - Methods for integrating data from the Port's CMDB into the support management processes to assist in reactive incident / problem investigation as well as proactive problem analysis.
  - Feasibility of using the Maximo application to support the service level management and problem management processes.

Capability Maturity Analysis

Recommendations (5)

IT Governance:

- ✓ Performance Management: Evaluate the business desire for formalized service level objectives and implement a service level management process based on these objectives. These objectives should be defined to align to the specific IT strategies defined for each business unit (e.g., IT as a utility provider vs. process optimizer).
- ✓ Risk Management: Continue to formalize the process for identifying and managing enterprise IT risks. The IT risk management process should be incorporated with the existing ICT Governance Board process and include the following attributes:
  - Define a comprehensive IT risk and control framework (e.g., based on CobiT) that addresses operational systems / processes as well as compliance and financial audit requirements.
  - Encompass the entire IT risk lifecycle, from initial identification and communication, through impact analysis and mitigation plan tracking.
  - Aggregate IT risks across IT (projects, departments, etc.) and provide a consistent basis for IT risk prioritization and analysis, potentially including methods for IT risk quantification.
  - Integrate with corporate risk management practices (e.g., internal audit, compliance).
- ✓ *(Beyond Target Goal)* - Resource Management: Consider Implementing a formal process for development and ongoing management of IT resource capabilities and skills. These efforts should include establishing skill development roadmaps for employees and working with Procurement to address improved use of temporary / contingency resources.

protiviti®

Appendices

protiviti®

Appendix A: IT Audit Risk Universe

Group or BU	Component/ Application / Process / Project	IT Risk Elements	Strategic / Planning	Organizational / Operational	Service / Marketplace	Financial	Regulatory / Legal Exposure	Data Integrity / Information (Sensitivity / Criticality)	Gross Risk Rating	Residual Risk Rating	Internal Control Environment
			10	25	20	15	15	15			
Aviation	Project	FIMS Phase II (2012)	7	8	8	3	6	9	700.0	544.4	4
ICT	Component	Data Center - Airport (C4)	5	9	7	8	7	7	745.0	579.4	4
Aviation	Component	Data Center - Toll Plaza	6	6	7	9	7	9	725.0	644.4	2
Aviation	Process	Project Management (Technology related)	7	8	7	6	6	5	665.0	591.1	2
Aviation	Application	Revenue Control (Parking System)	6	6	7	9	7	8	710.0	552.2	4
Aviation	Application	FIMS (Flight Information Management System)	7	8	9	4	4	8	690.0	536.7	4
ICT	Process	Business Continuity Planning	4	7	7	6	6	7	640.0	533.3	3
Aviation	Application	Physical Security System (Johnson Controls)	5	8	8	3	8	7	680.0	528.9	4
Aviation	Application	800 Mhz Communication System	6	8	6	4	8	7	665.0	517.2	4
Aviation	Process	Change Management - Aviation	5	7	6	6	6	6	615.0	512.5	3
Aviation	Process	Aviation Investment Steering Committee	7	7	7	7	6	5	655.0	509.4	4
ICT	Process	User Management	4	8	5	6	6	8	640.0	497.8	4
Aviation	Process	User Management	4	8	5	6	6	8	640.0	497.8	4
Aviation	Project	Access Control System Refresh (2013)	5	7	6	5	7	7	630.0	490.0	4
Aviation	Application	Anti-Virus (Trend Micro)	2	6	8	7	8	5	630.0	490.0	4
Aviation	Application	Train System	6	7	9	4	4	6	625.0	486.1	4
ICT	Component	PCI	4	4	4	6	9	9	580.0	483.3	3
Aviation	Process	IT Asset Management	4	6	6	7	6	5	580.0	483.3	3
ICT	Project	PeopleSoft Financials Upgrade (2012)	6	8	5	9	7	8	720.0	480.0	6
ICT	Process	Change Management - ICT	4	8	6	8	5	7	660.0	476.7	5
ICT	Component	Data Center - Fisher Plaza	4	8	6	7	6	7	660.0	476.7	5
Aviation	Component	Wireless Networking (AV)	5	7	7	4	6	6	605.0	470.6	4
Aviation	Application	Common-Use System (CUSE)	6	7	8	6	4	4	605.0	470.6	4
Seaport	Application	Propworks	4	7	6	7	5	6	605.0	470.6	4

high risk | Medium risk | Low risk | Must do

protiviti®

Appendix A: IT Audit Risk Universe (continued)

Group or BU	Component/ Application / Process / Project	IT Risk Elements	Strategic / Planning	Organizational / Operational	Service / Marketplace	Financial	Regulatory / Legal Exposure	Data Integrity / Information (Sensitivity / Criticality)	Gross Risk Rating	Residual Risk Rating	Internal Control Environment
			10	25	20	15	15	15			
Aviation	Application	Runway Taxi Systems	4	8	6	2	6	8	600.0	466.7	4
Aviation	Application	Loading Bridges	4	7	8	4	6	5	600.0	466.7	4
ICT	Process	Disaster Recovery Planning	5	7	8	7	7	7	700.0	466.7	6
Aviation	Application	Aviation Maximo	4	7	4	6	7	7	595.0	462.8	4
Aviation	Project	CUSE Migration (2012)	7	6	8	4	2	8	590.0	458.9	4
Aviation	Process	Vulnerability and Patch Management	4	6	7	7	7	6	630.0	455.0	5
Aviation	Application	ASDX (Approach Detection System)	3	9	4	2	5	9	575.0	447.2	4
ICT	Process	End-Point Security	3	7	6	7	8	8	670.0	446.7	6
ICT	Process	IT Governance Board	8	7	5	8	6	7	670.0	446.7	6
ICT	Process	Vulnerability and Patch Management	4	6	7	6	7	6	615.0	444.2	5
Aviation	Application	Propworks	6	6	6	7	4	5	570.0	443.3	4
ICT	Process	IT Training	4	7	4	4	7	7	565.0	439.4	4
Aviation	Application	ID Badge Winbadge Airport System	4	8	6	3	5	5	555.0	431.7	4
Aviation	Application	Noise Monitoring System	5	4	8	4	7	5	550.0	427.8	4
ICT	Project	Access Control System Refresh (2013)	6	7	6	5	7	7	640.0	426.7	6
Aviation	Application	Enterprise GIS	7	6	5	4	6	5	545.0	423.9	4
ICT	Component	Virus Protection	3	6	7	6	7	8	635.0	423.3	6
ICT	Process	IT Policy/Process Management	4	8	6	4	6	5	585.0	422.5	5
Seaport	Process	PMO	6	6	6	4	5	5	540.0	420.0	4
Aviation	Application	Airport Training System	5	6	5	3	7	6	540.0	420.0	4
ICT	Component	Wireless Security	4	6	6	6	7	8	625.0	416.7	6
ICT	Component	Database (SQL)	3	8	4	8	5	8	625.0	416.7	6
Aviation	Application	CUSS Kiosks & Reporting	7	5	8	5	2	5	535.0	416.1	4

high risk | Medium risk | Low risk | Must do

protiviti®

Appendix A: IT Audit Risk Universe (continued)

Group or BU	Component/ Application / Process / Project	IT Risk Elements	Strategic / Planning	Organizational / Operational	Service / Marketplace	Financial	Regulatory / Legal Exposure	Data Integrity / Information (Sensitivity / Criticality)	Gross Risk Rating	Residual Risk Rating	Internal Control Environment
			10	25	20	15	15	15			
Aviation	Application	Access Control Video System	4	7	4	4	6	6	535.0	416.1	4
ICT	Component	LAN/WAN	3	8	8	5	3	7	615.0	410.0	6
Aviation	Process	Physical Access (AV)	3	9	8	3	8	6	670.0	409.4	7
Aviation	Project	Elevators and Escalator Replacement	5	7	6	2	6	4	525.0	408.3	4
ICT	Project	Records and Document Management (2012)	3	7	5	5	8	7	605.0	403.3	6
Aviation	Process	Project Management Office (PMO)	7	8	6	7	6	5	660.0	403.3	7
ICT	Process	Project Management Office (PMO)	7	8	6	7	6	5	660.0	403.3	7
ICT	Application	E-Mail (Exchange)	5	9	8	2	7	6	660.0	403.3	7
ICT	Component	Active Directory Management	4	7	7	5	4	7	595.0	396.7	6
Aviation	Project	Safety Management System (Currently in RFP Process)	3	6	6	2	7	5	510.0	396.7	4
Aviation	Process	Aviation Communications Center (ACC)	4	7	7	3	7	6	595.0	396.7	6
Aviation	Application	Facility Management System (FMS)	3	7	4	4	6	5	510.0	396.7	4
ICT	Process	Backup and Recovery (i.e., Backup Replication, Deduplication)	4	5	4	6	7	7	545.0	393.6	5
Aviation	Process	Backup and Recovery	4	5	4	6	7	7	545.0	393.6	5
ICT	Project	Enhanced Client Security (Compliance Initiatives 2013)	4	5	7	6	7	6	590.0	393.3	6
ICT	Project	Security Checkpoint Wait Time (2012)	6	6	7	2	8	6	590.0	393.3	6
Aviation	Project	Airline Activity Management System (2012)	5	6	7	3	3	5	505.0	392.8	4
Seaport	Process	Physical Access (SeaPort)	3	7	6	2	6	4	505.0	392.8	4
Aviation	Application	Water Supply System	5	5	5	5	5	5	500.0	388.9	4
Police	Application	Public Safety CAD	5	5	5	5	5	5	500.0	388.9	4
Aviation	Application	Flight and Fleet	5	5	5	5	5	5	500.0	388.9	4
Seaport	Application	Marine Domain Awareness	5	5	5	5	5	5	500.0	388.9	4
Seaport	Project	Seaport Security Grant Round 7	5	5	5	5	5	5	500.0	388.9	4

high risk | Medium risk | Low risk | Must do

protiviti®

Appendix A: IT Audit Risk Universe (continued)

Group or BU	Component/ Application / Process / Project	IT Risk Elements	Strategic / Planning	Organizational / Operational	Service / Marketplace	Financial	Regulatory / Legal Exposure	Data Integrity / Information (Sensitivity / Criticality)	Gross Risk Rating	Residual Risk Rating	Internal Control Environment
			10	25	20	15	15	15			
Aviation	Application	Ground Transportation Management System	5	5	5	5	5	5	500.0	388.9	4
Fire Department	Project	Fire Systems Replacement	5	5	5	5	5	5	500.0	388.9	4
ICT	Process	IT Asset Management	4	6	6	7	6	5	580.0	386.7	6
ICT	Process	Release Management	3	7	3	6	5	7	535.0	386.4	5
ICT	Project	Maximo Enhancements and Upgrades (2012)	5	6	6	7	5	5	575.0	383.3	6
ICT	Component	Airport Garage Cameras	3	6	4	6	6	6	530.0	382.8	5
Aviation	Project	Time Clock System (2012)	2	7	2	6	5	6	490.0	381.1	4
ICT	Component	Port of Seattle Website	5	4	9	4	6	6	570.0	380.0	6
ICT	Project	Ground Transportation Management System (2012)	5	7	6	2	6	7	570.0	380.0	6
Seaport	Component	Wireless Networking (SeaPort)	5	6	5	4	5	6	525.0	379.2	5
Aviation	Application	Baggage System	3	6	7	5	3	3	485.0	377.2	4
ICT	Project	Cyber Security Info and Event Manager (SIEM)	4	5	5	6	7	7	565.0	376.7	6
ICT	Process	Incident Management	3	6	7	4	6	6	560.0	373.3	6
Aviation	Application	Voice Paging System	4	7	8	2	2	3	480.0	373.3	4
ICT	Component	Remote Access (VPN and Citrix)	3	7	4	4	7	7	555.0	370.0	6
Police	Application	Telestaff/Time Link	2	6	4	5	5	5	475.0	369.4	4
Fire Department	Application	Telestaff/Time Link	2	6	4	5	5	5	475.0	369.4	4
Seaport	Process	Emergency Management	4	6	7	2	4	6	510.0	368.3	5
ICT	Process	Network Security	3	6	5	4	7	7	550.0	366.7	6
ICT	Project	Internet Redesign	6	5	7	4	5	6	550.0	366.7	6
ICT	Process	Capital Requests	7	6	6	6	3	5	550.0	366.7	6
ICT	Process	IT Budgeting	7	6	6	6	4	4	550.0	366.7	6

high risk | Medium risk | Low risk | Must do

protiviti®

Appendix A: IT Audit Risk Universe (continued)

Group or BU	Component/ Application / Process / Project	IT Risk Elements	Strategic / Planning	Organizational / Operational	Service / Marketplace	Financial	Regulatory / Legal Exposure	Data Integrity / Information (Sensitivity / Criticality)	Gross Risk Rating	Residual Risk Rating	Internal Control Environment
			10	25	20	15	15	15			
ICT	Application	Microsoft Office Suite	4	9	4	7	4	6	600.0	366.7	7
ICT	Application	Maximo	4	7	4	6	7	7	595.0	363.6	7
ICT	Component	Telephony (PBX/VoIP)	4	8	7	2	4	5	545.0	363.3	6
ICT	Process	Service Desk	6	7	7	4	5	5	585.0	357.5	7
Cap Dev	Process	Contracting	4	6	6	6	5	4	535.0	356.7	6
Aviation	Process	Airport Training (e.g., Homeland Security Training, Security Training, Airfield Driver Training, Authorized Signatory Training, Fire Extinguisher Training)	5	6	7	2	7	4	535.0	356.7	6
ICT	Project	Common-Use Check In Kiosk Expansion (2012)	6	6	7	3	3	6	530.0	353.3	6
Cap Dev	Process	Service Level Agreement Management	6	6	4	5	7	4	530.0	353.3	6
ICT	Project	Propworks Upgrade (2012)	6	6	3	6	5	6	525.0	350.0	6
Aviation	Process	Emergency Management	4	7	8	2	5	6	570.0	348.3	7
ICT	Component	HIPAA	2	3	4	6	9	8	520.0	346.7	6
Corporate	Process	Physical Access (Corp)	3	7	6	3	6	4	520.0	346.7	6
ICT	Process	Systems, Networking and Infrastructure Monitoring	3	7	5	4	5	8	560.0	342.2	7
ICT	Project	Network Firewalls	3	6	3	4	7	7	510.0	340.0	6
Cap Dev	Process	Procurement (Central Procurement Office)	7	8	4	6	7	4	605.0	336.1	8
ICT	Application	PeopleSoft (Time Entry)	3	7	3	7	6	6	550.0	336.1	7
ICT	Application	System Center Configuration Manager (SCCM)	4	7	4	5	6	6	550.0	336.1	7
Aviation	Project	Automated Vehicle Identification Replacement	3	5	4	5	4	4	430.0	334.4	4
ICT	Project	CDS Replacement (2013)	5	5	5	5	5	5	500.0	333.3	6
ICT	Project	Computer Aided Dispatch Upgrade (2012)	5	5	5	5	5	5	500.0	333.3	6
ICT	Process	IT Strategic Planning	9	5	6	3	4	4	500.0	333.3	6
ICT	Application	Windows Operation System 7 Upgrade	3	7	4	5	5	7	540.0	330.0	7

high risk | Medium risk | Low risk | Must do

protiviti®

Appendix A: IT Audit Risk Universe (continued)

Group or BU	Component/ Application / Process / Project	IT Risk Elements	Strategic / Planning	Organizational / Operational	Service / Marketplace	Financial	Regulatory / Legal Exposure	Data Integrity / Information (Sensitivity / Criticality)	Gross Risk Rating	Residual Risk Rating	Internal Control Environment
			10	25	20	15	15	15			
ICT	Application	HP SiteScope (Service Desk)	4	7	4	4	6	6	535.0	326.9	7
ICT	Application	Nagios (Service Desk)	4	7	4	4	6	6	535.0	326.9	7
ICT	Application	Compass Intranet Application	4	6	3	4	6	6	490.0	326.7	6
ICT	Project	SharePoint Extranet	3	5	6	4	5	5	485.0	323.3	6
ICT	Application	FIM (File Integrity Monitoring - Tripwire)	3	6	3	5	6	8	525.0	320.8	7
ICT	Application	Tripwire SIM (Security Information and Event Management)	3	6	3	5	7	7	525.0	320.8	7
ICT	Process	SDLC	5	7	4	6	5	7	575.0	319.4	8
Cap Dev	Application	Sybase	4	6	3	6	5	7	520.0	317.8	7
ICT	Application	Oracle DB	4	6	3	6	5	7	520.0	317.8	7
Seaport	Project	Camera Installation	3	4	4	4	5	4	405.0	315.0	4
Aviation	Project	Camera Mapping with GIS	4	4	5	3	4	4	405.0	315.0	4
ICT	Project	ID Badge Software Upgrade (2012)	2	6	3	3	7	6	470.0	313.3	6
Aviation	Application	System Atlanta (i.e., Provides RVR readouts (barometric, air density, etc.)	2	7	2	2	4	5	400.0	311.1	4
Aviation	Application	Passer System (i.e. simulations that goes to about 20 miles out)	2	7	2	2	4	5	400.0	311.1	4
ICT	Process	Configuration Management	3	5	5	4	4	6	465.0	310.0	6
ICT	Component	Virtualization	7	6	3	3	4	8	505.0	308.6	7
Cap Dev	Application	Livelink Document Management	5	5	5	5	5	5	500.0	305.6	7
Cap Dev	Application	Contractor Data System	5	5	5	5	5	5	500.0	305.6	7
Corporate	Application	RiskMaster Claims & Risk Management	5	5	5	5	5	5	500.0	305.6	7
Corporate	Application	Budget System	5	5	5	5	5	5	500.0	305.6	7
Corporate	Application	eBilling Application	5	5	5	5	5	5	500.0	305.6	7
Corporate	Application	APS Scanning System	5	5	5	5	5	5	500.0	305.6	7
Cap Dev	Application	PMIS Project Management Information System	5	5	5	5	5	5	500.0	305.6	7

high risk | Medium risk | Low risk | Must do

protiviti®

Appendix A: IT Audit Risk Universe (continued)

Group or BU	Component/ Application / Process / Project	IT Risk Elements	Strategic / Planning	Organizational / Operational	Service / Marketplace	Financial	Regulatory / Legal Exposure	Data Integrity / Information (Sensitivity / Criticality)	Gross Risk Rating	Residual Risk Rating	Internal Control Environment
			10	25	20	15	15	15			
ICT	Application	Tableau (Data Mining)	7	5	4	5	4	6	500.0	305.6	7
Cap Dev	Process	Warranty Management	3	5	3	6	5	5	455.0	303.3	6
Aviation	Application	Veramark / Cable Management System	3	5	4	3	2	5	385.0	299.4	4
ICT	Application	SharePoint	3	7	3	5	4	6	490.0	299.4	7
Aviation	Project	Business Service Center	5	5	6	2	2	2	385.0	299.4	4
ICT	Project	Peoplesoft Self-Service (2013)	3	7	3	3	4	5	445.0	296.7	6
Cap Dev	Application	AutoCAD	6	6	4	4	3	6	485.0	296.4	7
Corporate	Component	Wireless Networking (Corp)	4	7	4	4	4	4	475.0	290.3	7
Cap Dev	Application	Bid Management System	4	5	4	5	5	5	470.0	287.2	7
ICT	Project	Budget System Upgrade (2013)	5	4	3	6	4	4	420.0	280.0	6
Corporate	Application	Concur	3	5	2	6	5	6	450.0	275.0	7
ICT	Application	Team Foundation Server (TFS)	2	5	3	4	5	7	445.0	271.9	7
ICT	Project	Police Records Management System (2012)	3	4	4	2	6	5	405.0	270.0	6
ICT	Project	Maintenance Management and Scheduling Tool (2012)	3	5	3	4	3	5	395.0	263.3	6
Corporate	Application	Send Word Now	3	4	5	2	6	5	425.0	259.7	7
Aviation	Process	Computer Refresh	3	5	4	2	2	2	325.0	252.8	4
ICT	Project	Enterprise Project Delivery System (2012) (Skire Unifier)	6	5	3	3	2	3	365.0	243.3	6
Aviation	Project	CUSS Kiosk Expansion	2	3	5	2	2	3	300.0	233.3	4
Corporate	Application	Plateau Learning Management System (LMS)	3	5	3	2	5	4	380.0	232.2	7
ICT	Application	Knowledgebase	3	5	5	2	2	4	375.0	229.2	7
ICT	Application	Self-Service Portal	3	5	3	2	2	3	320.0	213.3	6
ICT	Project	Rental Car/Bus Maintenance Facility (2012)	2	4	4	2	2	3	305.0	203.3	6
ICT	Component	Data Center - Pier 69	1	4	2	1	1	4	240.0	200.0	3

high risk | Medium risk | Low risk | Must do

protiviti®

Appendix B: Benchmarking Overview

Benchmark information presented in this report is primarily based on research conducted by the following three organizations:

IT Process Institute

- ✓ Organization Overview
- ✓ IT Controls Performance Study
- ✓ IT Strategic Alignment Study

Gartner

- ✓ Organization Overview
- ✓ IT Key Metrics Data 2012: IT Spending and Staffing Report

Appendix B: Benchmarking Overview

About the IT Process Institute

The IT Process Institute (ITPI) is a not-for-profit organization formed by IT practitioners and academics (Carnegie Mellon, FSU) that supports IT audit, security, and operations professionals

Focus: Research, benchmarking, and prescriptive guidance

Goal: To measurably enhance efficiency & effectiveness of IT operations & controls

Approach: Pairing industry based volunteers with leading university researchers, to identify and study top performing IT organizations

The Visible Ops Handbook and Visible Ops Security

- Based on 5 years studying high-performing IT Operations & Security organizations
- 100 pages long, dense type but easy to read – Over 50,000 copies in print
- First published in 2004, revised with new content & published again in 2005 / 2007
- Owned by the ITPI, jointly developed by IT practitioners and academic research

IT Controls Performance Study & Benchmark Survey

- 330 North American enterprises
- Designed to evaluate the performance impact of IT Controls.
- Assumes "controlled" process performs better and defines by how much
- Answer questions about which IT Controls efforts have the greatest impact

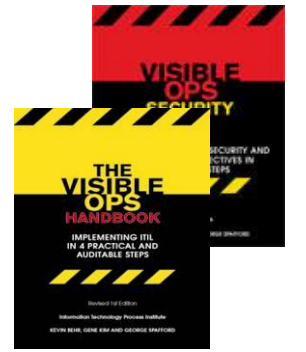
Change, Configuration, and Release (CCR) Performance Study & Benchmark

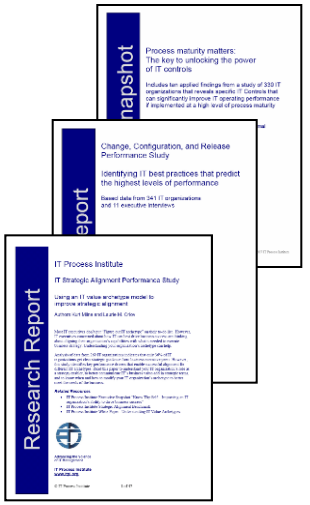
- Building on ITCP Study findings, 341 companies surveyed
- Identified 12 leading practices from 57 common approaches to CCR
- 7 sets of practices statistically predict performance improvements

IT Strategic Alignment Performance Study & Benchmark

- Building on ITCP and CCR Study findings, 269 companies surveyed
- Identified 3 major IT strategic models and key practices / challenges for each
- 5 sets of practices that directly impact alignment performance

Information Technology Process Institute





protiviti®

Appendix B: Benchmarking Overview

ITPI IT Controls Performance Study

Goals and Assumptions

- ✓ Designed to evaluate the performance impact of IT Controls
- ✓ Assumes "controlled" process performs better and defines by how much
- ✓ Answer questions about which IT Controls efforts have the greatest impact

The following slides provide additional Information related to this Benchmark Study

protiviti®

Appendix B: Benchmarking Overview

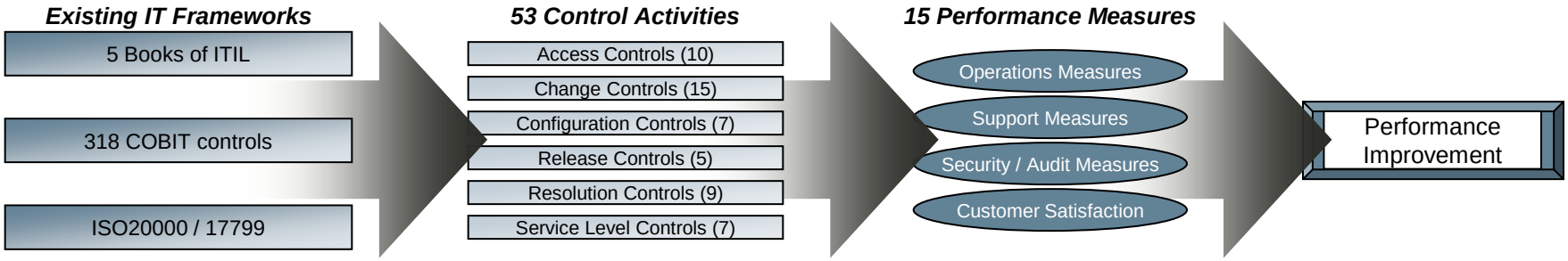
ITPI IT Controls Performance Study Key Facts

Study Demographics . . .

- ✓ 330 North American companies represented
- ✓ Average IT expenditure: $96.8 million
- ✓ Mean number of IT employees: 656
- ✓ 85% of organizations have 1000+ employees
- ✓ 37% have 10,000+ employees
- ✓ A broad range of revenue / operating budgets:
  - 42% between $250M and $1B,
  - 41% between $1B and $10B, and
  - 14% from companies with >$10B

Study Details . . .

- ✓ Benchmark surveys completed Dec06 / Jan07
- ✓ 53% of respondents are IT Director, VP or CXO
- ✓ 89 total questions:
  - 13 Demographic Questions
  - 53 Control Activity Questions
  - 12 General IT Effectiveness Questions
  - 11 Specific Control Performance Questions
- ✓ New Control Maturity (Likert) Scale



ITPI Controls Performance Study – Research Approach

1: Cluster participants by control use & performance

2: Identify Foundational Controls that best predict performance variation

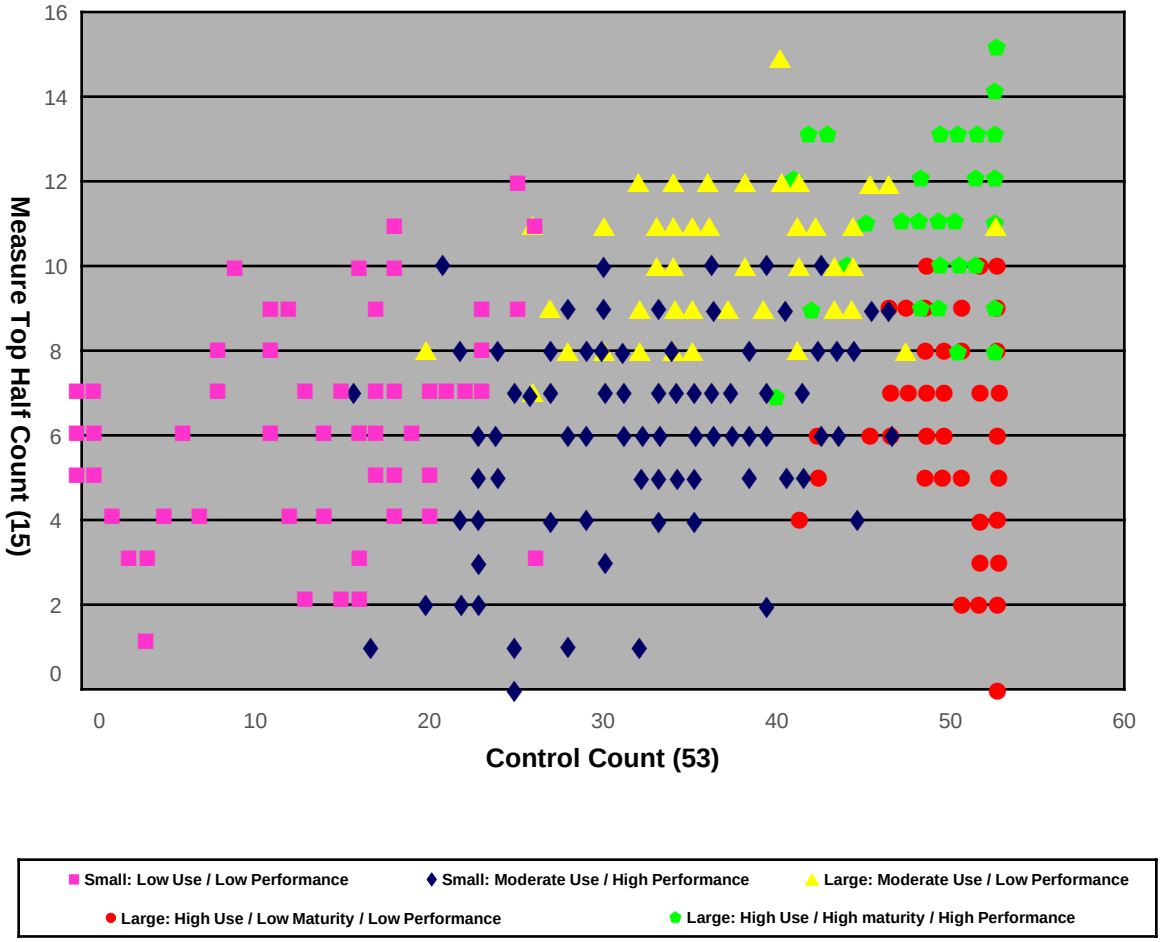
3: Assess impact of control process maturity

4: Quantify performance improvement potential

protiviti®

Appendix B: Benchmarking Overview

ITPI IT Controls Performance Study - Analysis Approach



Basic Analysis:

5 Performance Clusters are evident, with:

- Similar maturity of controls
- Distinct profiles of IT performance

…but there is no single determinant of performance!!

Several important trends:

- No companies with low control maturity had high IT performance
- IT Controls affect performance *differently* at Small vs. Large companies
- Control Maturity matters, *especially* in Larger companies

protiviti®

Appendix B: Benchmarking Overview

ITPI IT Controls Performance Study - Foundational Controls (Smaller Organizations)

Research Question:

What subset of controls impact smaller organization performance the most?

Methodology:

Use regression to determine relationship between controls and performance for two smaller organization clusters with Low and Moderate control use

Findings:

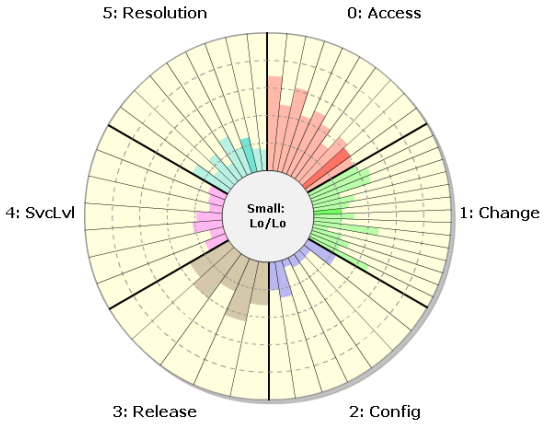
Three controls predict 45% of performance variation in smaller organizations with Low to Moderate control use:

1. A defined process to detect unauthorized access
2. Defined consequences for intentional, unauthorized changes
3. A defined process for managing known errors

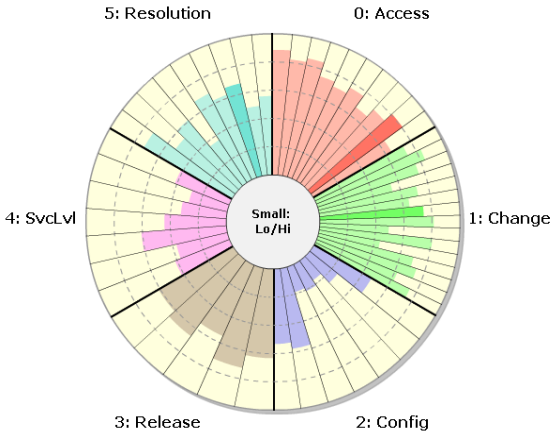
Important Note:

In this Study, there is no single, distinct boundary between "Smaller" and "Larger" companies – the distinction found was between companies that tended to "use" more controls *(with a tendency to be "Large")* and those that did not *(with a tendency to be "Small")*

Low Use / Low Perf. (18%)



Moderate Use / High Perf. (14%)



protiviti®

Appendix B: Benchmarking Overview

ITPI IT Controls Performance Study - Foundational Controls (Larger Organizations)

Research Question:

What subset of controls impact larger organization performance the most?

Methodology:

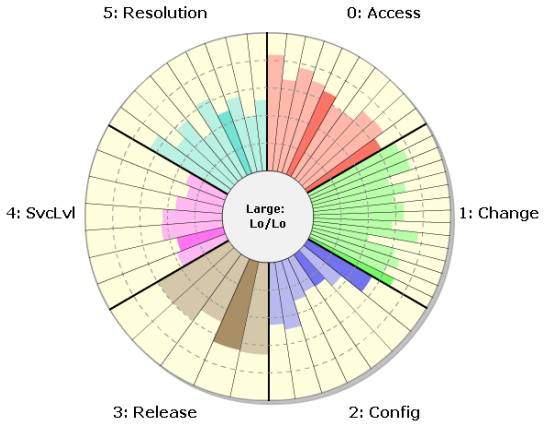
Use regression to determine relationship between controls and performance for two larger organizational clusters

Findings:

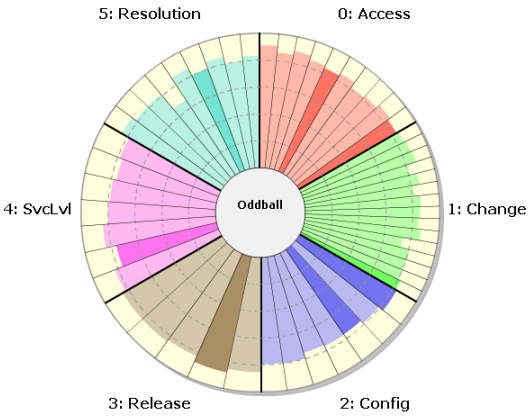
Nine foundational controls predict 60% of performance variation in larger organizations

1. A defined process to analyze & diagnose root cause of problems
2. Provide IT personnel with accurate information about the current configuration
3. Changes are thoroughly tested before release
4. Well-defined roles and responsibilities for IT personnel
5. A defined process to review logs of violation and security activity to identify and resolve unauthorized access incidents
6. A defined process to identify consequences if service level targets are not met
7. A defined process for IT configuration management
8. A defined process for testing releases before moving to the production environment
9. CMDB describes the relationships and dependencies between configuration items (infrastructure components)

Moderate Use / Low Perf. (35%)



High Use / Low Perf. (19%)



protiviti®

Appendix B: Benchmarking Overview

ITPI IT Controls Performance Study - Assess impact of control process maturity

Research Question:

Does process maturity explain performance difference between two larger organization clusters – both with High control use – but different levels of performance?

Methodology:

Test control use and control maturity measures to determine if they are statistically different for these two groups.

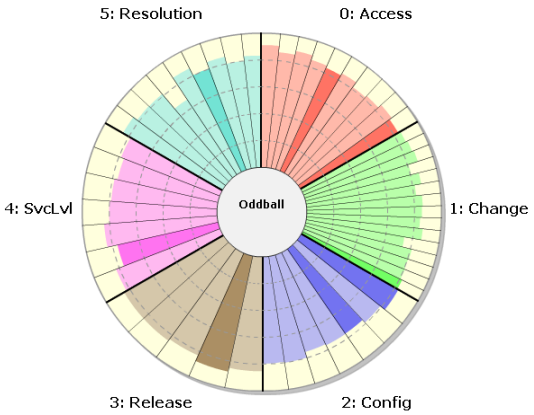
- Group respondents by performance, and assess various maturity measures for practical use
- Count of foundational controls at process maturity level 4 and 5 had strongest correlation with performance

Findings:

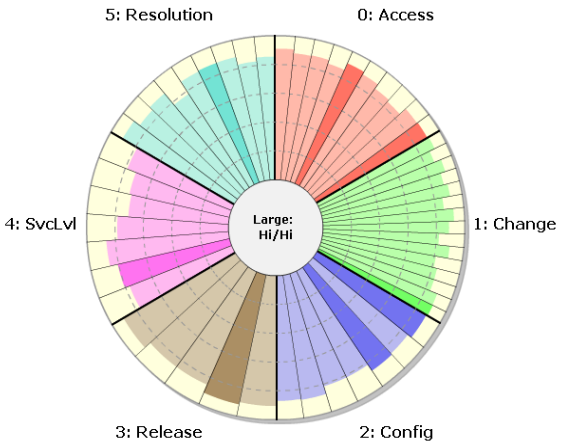
Both overall control maturity and foundational control maturity are statistically higher for high performing cluster:

- Process maturity explains – in part – the difference in performance of these two organization types
- Possible Conclusions:
  - Foundational IT controls should be implemented at higher level of process maturity in order to achieve performance improvement
  - Some Process should be monitored for exceptions, and exceptions should be managed with consequences

High Use / Low Perf. (19%)



High Use / High Perf. (14%)



protiviti®

Appendix B: Benchmarking Overview

ITPI IT Controls Performance Study - Performance Improvement Potential

In relation to Low and Medium Performers, Top Performers can generally:

- Authorize and implement 5 - 14 times more IT changes
- Increase the number of successful changes by 11% - 25%
- Support 2.6 - 6.6 times more software applications per IT staff
- Support 1.3 - 1.9 times more servers per System Administrator
- Increase customer satisfaction by 18% - 30%
- Automatically detect 12% - 76% more potential security breaches

At the same time, Top Performers experience a reduction in:

- Time spent to repair large IT system outages by 35%–58%
- The number of "emergency" change requests processed by 29%–55%
- The number of late projects by 20% - 50%
- Unplanned IT work by 12% - 37%
- Repeat audit findings by 39% - 52%

A significant portion of performance differential is due to Foundational Control Use

protiviti®

Appendix B: Benchmarking Overview

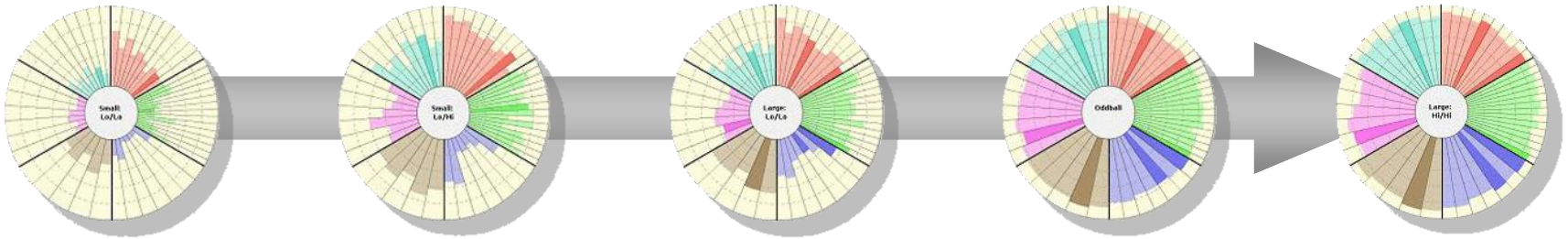
ITPI IT Controls Performance Study - Key Findings Summary & Conclusions

- Controls impact smaller and larger organizations differently
- Three Foundational Controls predict 45% of the performance variation in ***Smaller*** organizations
- Nine Foundational Controls predict 60% of the performance variation in ***Larger*** organizations
- Organizations should monitor and manage process exceptions for Foundational Controls in order to achieve performance improvement
- Performance improvement potential is significant

Top Performers get *more* done with *less*…

Top Performers have *much fewer* audit & regulatory issues…

…and the cost savings associated with improvements such as reduced unplanned work, increased change success and higher first-fix rates goes *directly to the bottom line*



protiviti®

Appendix B: Benchmarking Overview

ITPI IT Strategic Alignment Study

Basic Question:

How can organizations manage IT for competitive advantage?

Focus:

Determine the specific practices that enable IT strategic alignment success.

Study Approach:

- ✓ Cluster participants into one of three IT Value Archetypes based on answers to nine attribute questions
- ✓ Identify alignment challenges faced by each archetype
- ✓ Identify practices that optimize strategic alignment for each archetype
- ✓ Establish recommendations on how organization's can transition to other archetypes

protiviti®

Appendix B: Benchmarking Overview

ITPI IT Strategic Alignment Study - Key Facts

Study Demographics:

- ✓ 269 North American companies represented across various industries
- ✓ Respondent company annual revenues greater than $100 million
  - 33% - $100M to $250M
  - 34% - $251M to $1B
  - 21% - $1B to $10B
  - 12% - >$10B
- ✓ IT managers and executives
  - 21% - Managers
  - 42% - Directors
  - 33% - VP / Executive
  - 4% - Individuals

Study Details:

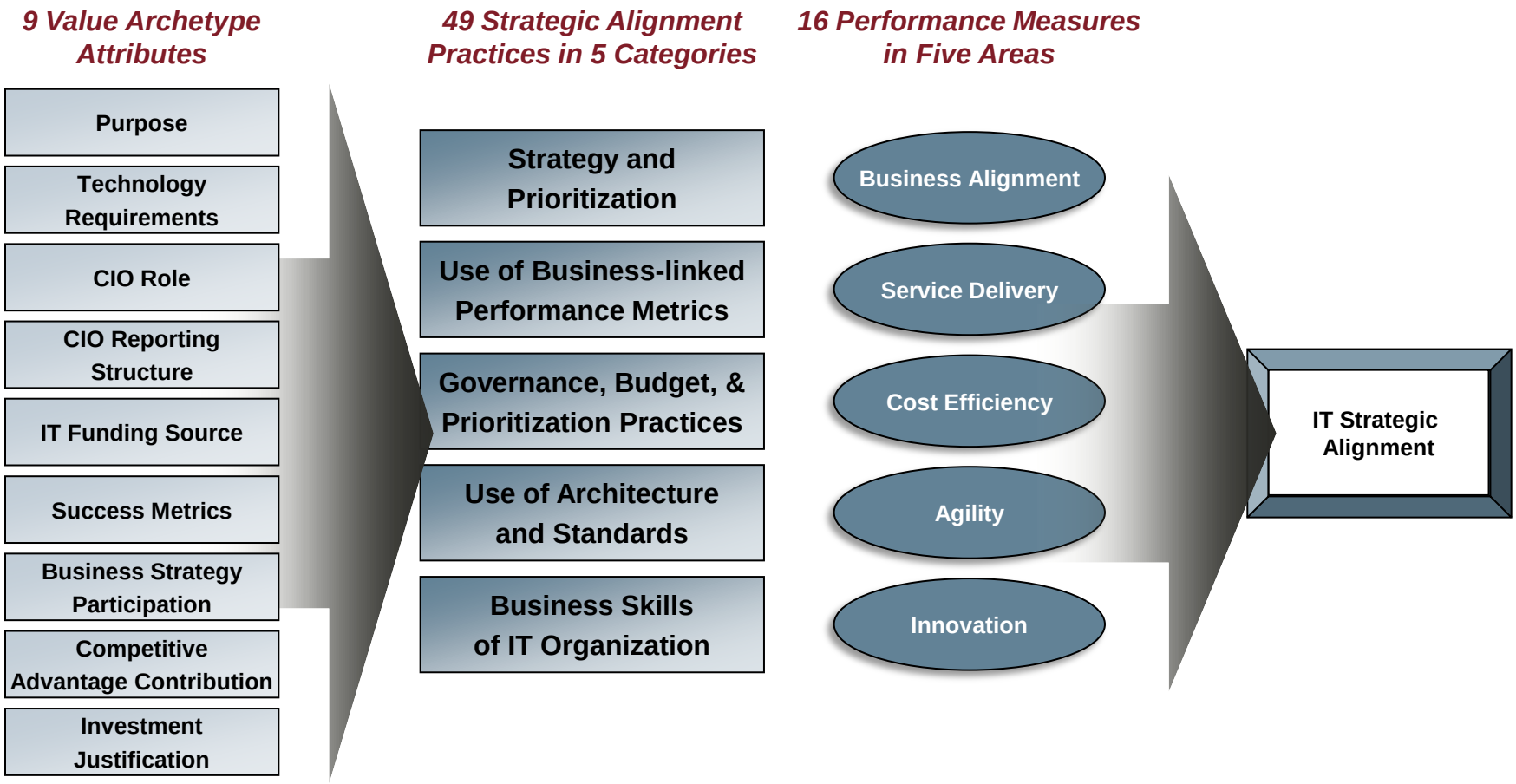
- ✓ Benchmark surveys completed October 2007
- ✓ 49 alignment practices
  - Strategy / Prioritization
  - Use of business-linked performance metrics
  - Governance, Budget, and Prioritization practices
  - Use of common architecture / standards
  - Business skills of IT organization
- ✓ 16 alignment measures on 1-10 scale
  - Business Alignment
  - Service Delivery
  - Cost Efficiency
  - Agility
  - Innovation

protiviti®

Appendix B: Benchmarking Overview

ITPI IT Strategic Alignment Study - Measuring Activities & Performance

How did the ITPI determine what data and performance measures to study?



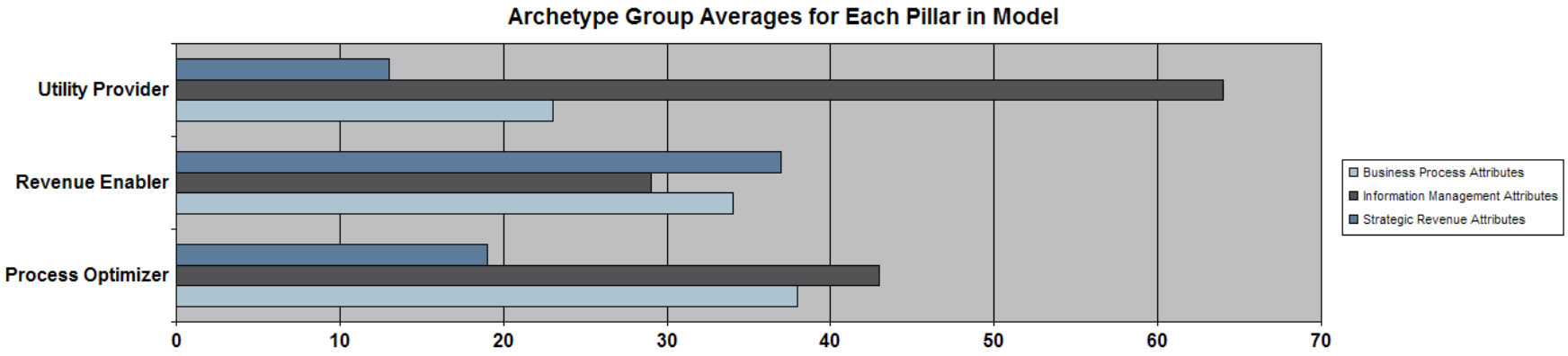
protiviti®

Appendix B: Benchmarking Overview

ITPI IT Strategic Alignment Study - The Three IT Value Archetypes

Study participants were placed into one of three IT value archetypes based on their answers to nine attribute questions. The IT value archetypes are:

- ✓ ***Utility Providers*** are not actively engaged with the business. They focus primarily on providing shared information management services.
- ✓ ***Process Optimizers*** are responsive to the business. They focus on shared information management services plus business applications and business process optimization.
- ✓ ***Revenue Enablers*** are well integrated into the business. They focus on shared information management services, business process optimization, and technology-enabled products and services.



protiviti®

Appendix B: Benchmarking Overview

ITPI IT Strategic Alignment Study - Key Takeaways

The study revealed that:

- ✓ Mixed objectives suggest that ***each archetype group requires scaled sets of competencies*** as the organization focuses on more than shared information management services.
- ✓ Specific technologies, IT strategies, and best practices ***do not apply equally well to all business strategies in all organizations***.
- ✓ Practice alignment can be assessed only after ***verifying that the current IT archetype fits appropriately with the current business strategy***.

Further, there is a distinction between **Business Alignment** vs. **Business Integration**

- ✓ ***Revenue Enablers*** have the highest alignment performance scores:
  - They are tightly integrated with the business
  - They have the least control over their budget, but have the highest budget growth
- ✓ ***Utility Providers*** have the lowest alignment performance scores:
  - They are more loosely aligned with the business
  - They have the most control over their budget, but have the lowest budget growth

protiviti®

Appendix B: Benchmarking Overview

About Gartner

- ✓ Founded in 1979, Gartner is Technology focused research organization. The Company consists of Gartner Research, Gartner Executive Programs, Gartner Consulting and Gartner Events.
- ✓ Gartner's primary audience is Chief Information Officers and other Senior IT Executives.
- ✓ Stats / Sizing
  - 3,700 associates, including 1,200 research analysts and consultants in 75 countries worldwide.
  - Serves 10,000 clients
  - 2005 Revenue – US $989 Million

protiviti®

Appendix B: Benchmarking Overview

Gartner IT Key Metrics Data

The Gartner IT Key Metrics Data reports contain important database averages from a subset of metrics and prescriptive engagements available through Gartner Benchmark Analytics. These database averages do not account for individual variations of unique competitive landscape, business scale, IT complexity or demand which may be justified by specific business needs. Complexity and demand for IT services should always be considered in the context of a cost or performance evaluation as these factors often dictate long term support requirements. IT Key Metrics Data should be used as a high level directional indicator and in the creation of planning assumptions and not viewed as an absolute benchmark. The 2012 IT Key Metrics Data: IT Spending and Staffing Report was used for Protiviti's analysis (prior year metrics reports were used for multi-year trending analysis).

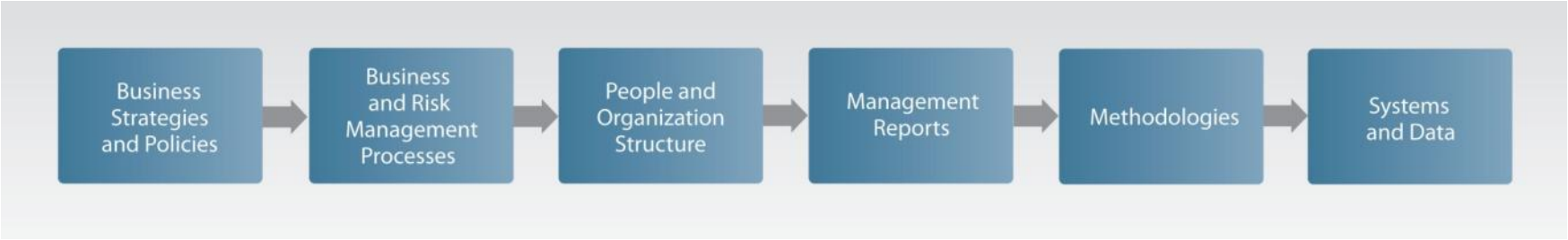
Key Findings

- ✓ Average IT spending across all industries increased by 4.4% in 2011 and is expected to increase by a further 4.7% in 2012.
- ✓ From 2010 to 2011, average IT spending as a percent of revenue increased from 3.5% to 3.6%, and IT spending as a percent of operating expense increased from 4.3% to 4.5%. In 2012, IT spending as a percent of revenue and IT spending as a percent of operating expense are expected to drop to 3.2% and 4.0%, respectively.
- ✓ IT spending per employee, at $12,708, rose by 2.9% compared to 2010, and it returned to a value similar to that seen in 2009.
- ✓ IT full-time equivalents (FTEs) as a percent of total employees, at 5.3%, remained nearly unchanged since 2009.

Appendix C: Six Elements of Infrastructure

The Building Blocks of Maturity

The other model used to evaluate Capability Maturity is Protiviti's "Risk Management Infrastructure" model, which demonstrates the business components of a quality process.

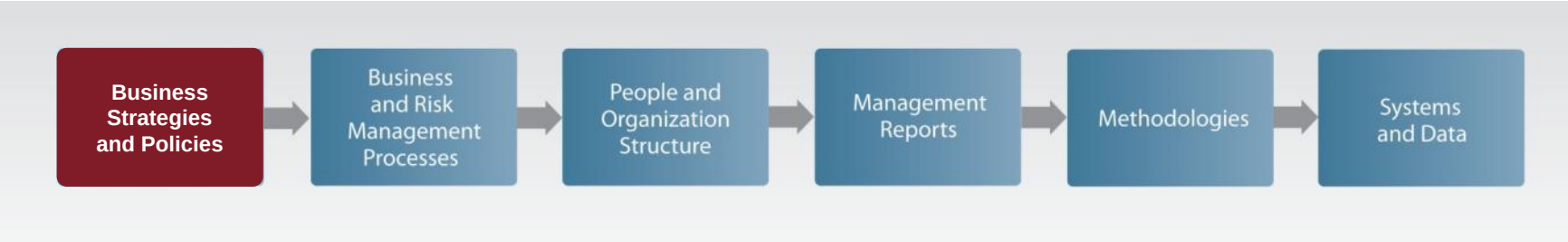


The "6 Elements of Infrastructure"

- ✓ Describes the components needed to ensure quality & risk management
- ✓ Are generally designed from left to right as shown above
- ✓ Each component contributes to the overall process maturity of each area
- ✓ Describes the "necessary ingredients" for mitigating risk to strategies the business deems critical

protiviti®

Appendix C: Six Elements of Infrastructure



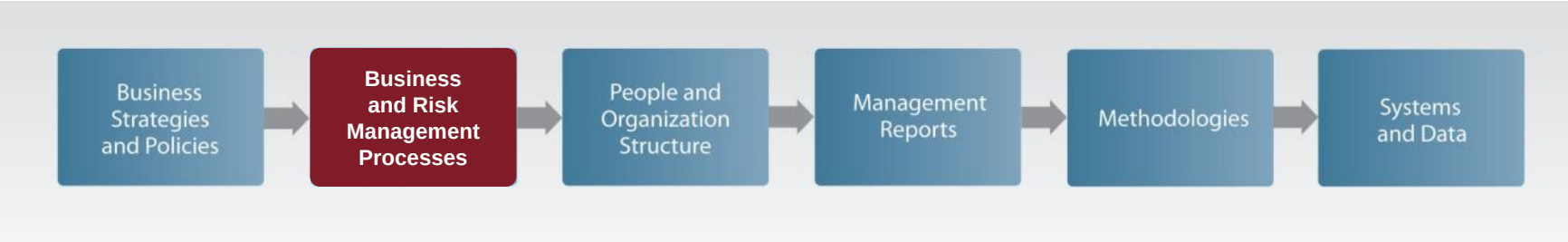
In this component of the Six Elements, the formal Business Policy framework includes specific guidelines as well as the more general principles that apply to all aspects of the business and management of its risks. Policies enable process owners to understand what the organization intends to accomplish with a process. Policies are linked to strategy; they put strategy in play.

These policies:

- ✓ Articulate the selected process objectives so that process owners and personnel will understand what the risk management capabilities are intended to accomplish.
- ✓ Guide management and process owners toward achieving specific process goals, implementing specific risk strategies, designing specific processes, using designated products, executing specific transaction types, and complying with specific risk tolerances and expected standards of conduct.
- ✓ Help senior executives and the Board clarify their understanding of the process and the related impact on the business.

protiviti®

Appendix C: Six Elements of Infrastructure



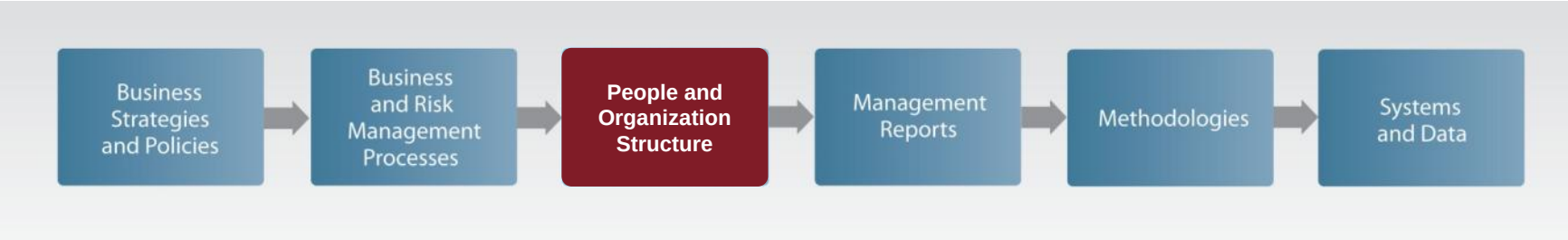
In this component of the Six Elements, Business Processes:

- ✓ Are the primary means of executing business strategies and policies.
- ✓ Contain inputs, activities and outputs that are integrated with business processes.
- ✓ Should contain operational risk controls that are built into day-to-day processes.
- ✓ Are the sequence of activities and tasks that must be performed and are described precisely by process owners to achieve the desired process objectives.
- ✓ Promote a clearer understanding of the activities requiring the most attention from a risk management and control standpoint.
- ✓ Risk responses and control activities are desirably integrated within business processes because risks are best managed and controlled as close as possible to the source.

This risk element is deficient if the process does not carry out established policies or achieve the intended result.

protiviti®

Appendix C: Six Elements of Infrastructure



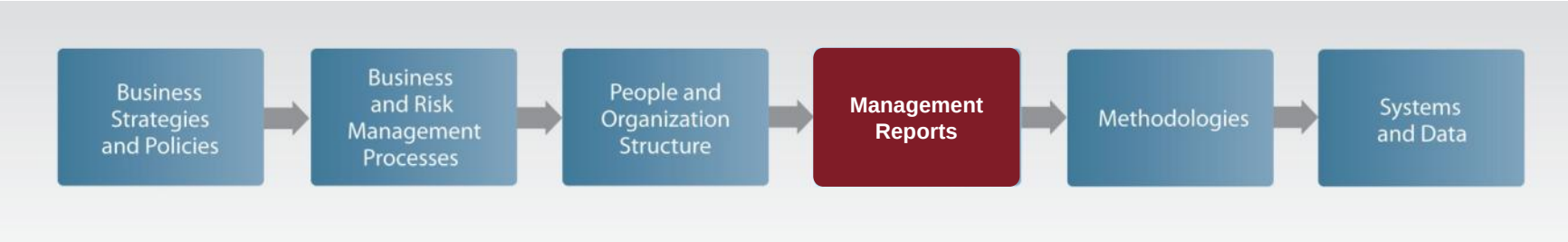
In this component of the Six Elements:

- ✓ People execute processes.
- ✓ Key tasks are assigned to people with the necessary knowledge, skill, and expertise.
- ✓ As people take on new risk management responsibilities, their roles, accountability and relationships with other risk owners should be clearly defined.
- ✓ Process owners should be satisfied that everyone's job is clearly spelled out so that they can hold people accountable, both within and outside the organization.
- ✓ Roles and responsibilities of risk-taking versus risk-monitoring functions should be clearly defined and delineated.
- ✓ Process owners are accountable for losses experienced with undesirable risk incidents occur.
- ✓ Key tasks are assigned to people with the requisite knowledge, skill, and expertise. Roles and responsibilities of risk-taking versus risk-monitoring functions must be defined and delineated.

This risk element is deficient if people lack the knowledge and experience to perform the process.

protiviti®

Appendix C: Six Elements of Infrastructure



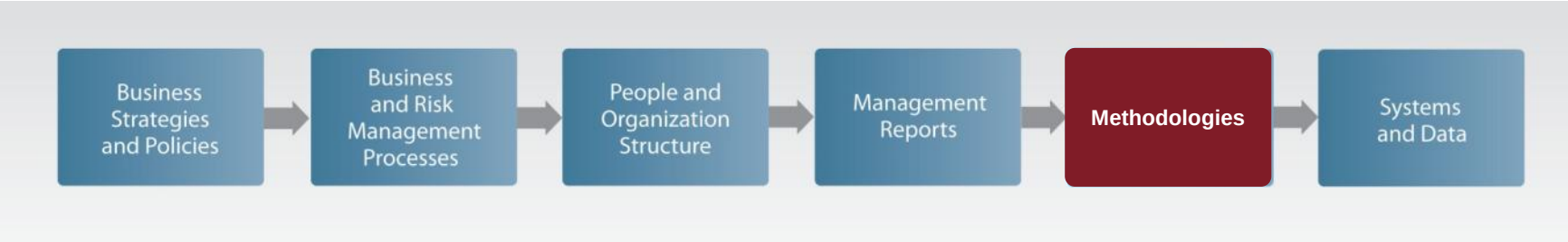
In this component of the Six Elements:

- ✓ Reports should be actionable, easy to use and linked to well-defined accountabilities.
- ✓ Reports are designed according to the information needs of people who are responsible for executing processes in accordance with the risk strategy.
- ✓ Personnel with risk management responsibilities use reports to monitor achievement of objectives, execution of strategies, and compliance with policies.
- ✓ Management reports include position reports, transaction reports, management and board reports, valuation / scenario analyses and comprehensive reports.
- ✓ Factors to consider when reporting on frequency include the volatility or severity of the risks, the needs for the user and the dynamics of the underlying business activities.
- ✓ Reporting on risks is integral to an organization's success as reporting on quality, costs, and time.

This risk element is deficient if reports do not provide enough information for management.

protiviti®

Appendix C: Six Elements of Infrastructure



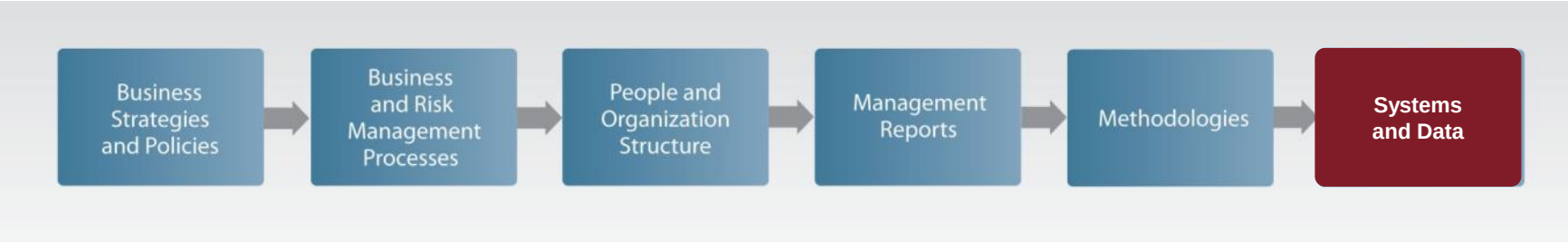
Methodologies organize key tasks and a working body of knowledge within a logical, well-structured framework. Effective methodologies help managers:

- ✓ Identify, quantify and prioritize risks.
- ✓ Source risk to its root causes and key drivers.
- ✓ Support the analysis of risk / reward trade-offs and portfolio diversification.
- ✓ Price products and services to adequately compensate for risks undertaken.
- ✓ Evaluate cost effectiveness of risk mitigation alternatives and allocation of capital to absorb potential losses.

This risk element is deficient if methodologies do not adequately analyze data and information.

protiviti®

Appendix C: Six Elements of Infrastructure



In this component of the Six Elements, Systems and Data:

- ✓ Support the modeling and reporting that are integral to risk management capabilities.
- ✓ Provide relevant, accurate, and on-time information.
- ✓ Should meet the company's business requirements, and be flexible enough to allow for future enhancement, scalability and integration with other systems.

Systems and data typically include:

- ✓ Transaction systems and analytical software.
- ✓ Systems that identify and capture risk drivers.
- ✓ Systems and databases that warehouse key data elements relating to specific tasks.
- ✓ Special-purpose systems that quantify individual risks and aggregate portfolios of risks or provide risk analytics.

This risk element is deficient if information is not available for analysis and reporting.

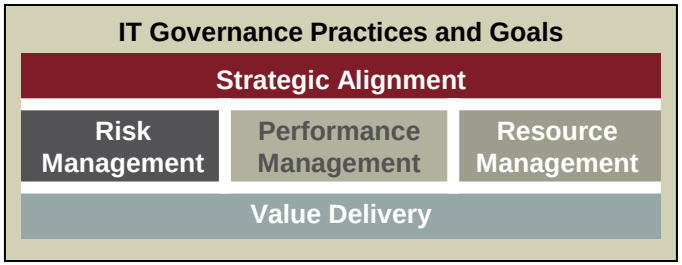
protiviti®

Appendix D: Five Elements of IT Governance

Strategic Alignment

Objective:

Determine if a relationship exists between IT and business objectives and if this relationship has been established through participation between both IT and business management.



Example Review Documents:

- IT Strategic Plan
- Third Party service provider agreements and RFP process

Typical Areas of Concern:

- Is IT management aware of the overall business strategy?
- What is IT's involvement in defining the business strategy?
- Do current IT initiatives relate to one or more of the organization's strategic objectives?
- Is there a clear line of communication between IT and business management?
- How do third party service providers support business objectives?
- What IT archetype is necessary to support the business objectives?

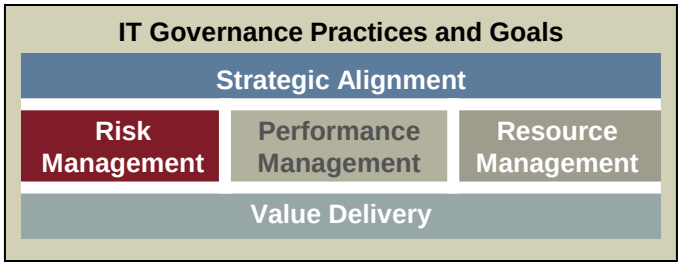
protiviti®

Appendix D: Five Elements of IT Governance

Risk Management

Objective:

Determine if activities are conducted relating to the identification and analysis of risks impacting the achievement of business objectives and the preparation of financial statements.



Example Review Documents:

- Business Continuity and Disaster Recovery Plans and Test Results
- IT Risk Assessment
- Third Party Service Provider Agreements and Request For Proposal Policies and Procedures

Typical Areas of Concern:

- Is a process in place to assess, address, and communicate IT risks to key stakeholders and executive management during the project, change, and release management processes?
- How does IT select and manage third party vendor relationships?
- Does a business continuity and disaster recovery plan exist and is it tested on a periodic basis?
- Does a risk management plan exist and are risk management activities incorporated into project, change, and release management process?
- Do discussions between IT, Business, and Compliance leadership occur in order to identify ways in which the IT environment can assist in strengthening the organization's control environment?

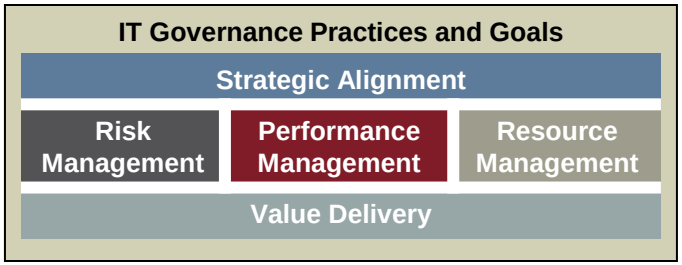
protiviti®

Appendix D: Five Elements of IT Governance

Performance Management

Objective:

Determine if the effectiveness of IT systems, processes, and personnel, internal and external, are being monitored for alignment with business needs.



Example Review Documents:

- Performance metrics for services, projects, processes, and systems
- Reports of IT's performance against defined metrics to key stakeholders and executive management
- Third Party Service Level Agreements
- Incident and Problem Management Policies and Procedures
- Cost Allocation Policies and Procedures

Typical Areas of Concern:

- Does the IT organization report performance metrics to key stakeholders?
- Are processes in place to review key performance metrics and correct items falling below a reasonable level?
- Do performance management activities consider both internal and third party IT activities?
- Is IT performance reported in IT or Business terms? Are the metrics operational, strategic, or both?
- Is a process in place to establish performance metrics based on changing business needs?
- Do the Board of Directors and Executive management have an awareness of IT performance based on quantifiable data?

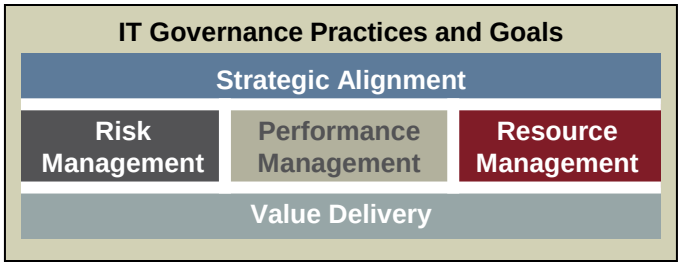
protiviti®

Appendix D: Five Elements of IT Governance

Resource Management

Objective:

Determine if adequate activities are being performed to align the use of resources (applications, information, infrastructure, people) to meet the needs of the business.



Example Review Documents:

- IT Organization Chart
- IT Job Descriptions
- Sourcing Strategy for IT projects
- IT Segregation of Duties Requirements
- IT Asset Management Policies and Procedures

Typical Areas of Concern:

- Are processes in place to assess and implement IT segregation of duties?
- Has an IT sourcing strategy been established that align with business objectives?
- Do IT resource dedicate more time to operational or strategic objectives?
- Does the IT department have processes in place to facilitate knowledge sharing within the department and with the business?
- Have IT resources (employees, applications, hardware) been optimized to support business objectives?
- Have formal job descriptions and reporting relationships been created and communicated for all IT positions?
- Has an asset management program has been established?

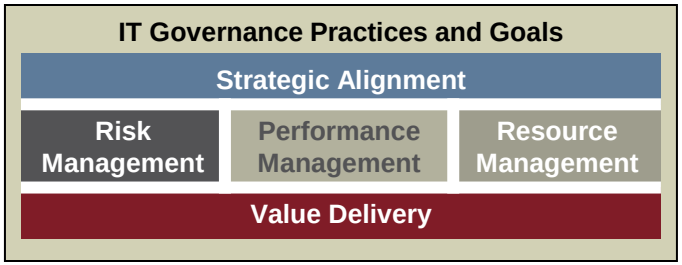
protiviti®

Appendix D: Five Elements of IT Governance

Value Delivery

Objective:

Determine if IT is effectively managing costs as they relate to meeting business objectives and communicating this management to the appropriate individuals.



Example Review Documents:

- IT Steering Committee Meeting Minutes
- Policies and Procedures for the Development and Management of IT projects
- IT Budget

Typical Areas of Concern:

- Is there a clear relationship between IT project performance indicators and business objectives?
- Has the IT budget been communicated to business leadership? Does business leadership understand the investments that have been made in IT?
- Does IT actively communicate the expected and realized value of IT projects?
- Does the business rely on the integrity and accuracy of data captured and reported by IT systems?
- Do IT and business leaders meet on a periodic basis to review the current and upcoming IT initiatives to reassess alignment with business objectives?

protiviti®

Appendix E: Capability Maturity Model Matrices

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 nor 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

Typical Target Zone

increased Costs

Current Maturity

Partial Demonstration

Target Maturity

Appendix E: Capability Maturity Model Matrices

Continuity Management

	Strategy & Policies	Processes & Controls	People & Organization	Management Reports	Methodologies	Systems & Data
Optimizing	Business continuity management (BCM) is advertised internally and externally as a competitive advantage; BCM is used to drive strategic goals and internal efficiencies	Comprehensive, organization-wide BCM processes are aligned with strategic objectives and customer expectations; World-class process performance	BCM operates as a core business function, chartered with clear accountability and responsibility; Personnel are well trained regarding their roles and duties	Relevant information regarding key threats and impacts are available with little notice; Continuity reporting is a normal part of operations	BCM analysis is continuously and systematically improved; Continuity risks are analyzed in relation to strategic decisions	BCM program is aligned with enterprise systems in near real time; New technologies are pursued to ensure BCM success; BCM program leverages enterprise data to improve BCM
Managed	BCM policy and objectives are ingrained into IT governance practices; Service measures designed into BCM processes and testing schemes	Threats understood and proactively managed; BCM practices address recovery objectives and regulatory compliance; BCM processes formalized and plans well maintained	Dedicated department maintains plan content & conduct tests and exercises; Cross-training limits points-of-failure; Clear process ownership and management support	BCM program effectiveness reported to and understood by upper management; Reporting is used to ensure recovery objectives are met and to improve BCM plans	BCM data is analyzed in the context of overall risk; Enterprise risk assessments include BCM-related analysis. Analysis incorporates special circumstances.	Information regarding BCM risk is readily available and used by line of business managers as well as BCM program managers
Defined	Policy and strategy define objectives for success; Recovery processes are formally defined and integrated into the BCM program	Formal BCM process or lifecycle has been designed and deployed; Risk assessment and business impact analysis have been performed	Roles have been created for those responsible for BCM and IT DR; process ownership established with widespread training and awareness	All key measures analyzed periodically; Metrics require some refinement; Service thresholds established; Processes in place to keep BIA current	Regulatory or industry planning standards consistently integrated into risk mitigation and BCM program	Continuity information is collected in a systematic way that can be leveraged across departments; Data is available for key BCM decisions
Repeatable	IT disaster recovery (DR) planning is the focus; Testing focused on component recovery; BCM is decentralized	The organization's BCM processes include crisis management, business resumption or IT DR	BCM and IT DR are part-time roles, exist in silos, and unintegrated; limited training	Reporting tactical; Reports may be distributed indiscriminately	Basic models are inconsistently utilized; Analysis is limited/isolated	Some issues such as IT DR collect relevant data but it is isolated, not comprehensive, and not shared
Initial	Focus is data backup; Processes developed in silos; Expectations are undefined without risk assessment	BCM is ad-hoc; A formal plan does not exist for testing or awareness	BCM ownership not clearly defined or simply added to the role of IT operators; Success depends on heroics	BCM reporting non-existent; Only anecdotal evidence available; Lack of confidence in the ability recover	"Best effort" is employed for a methodology and "best guess" is used to identify business requirements	Very limited ability to collect data on the BCM program other than direct management of continuity vendors

increased Costs

Typical Target Zone

increased Costs

Current Maturity

Partial Demonstration

Target Maturity

Appendix E: Capability Maturity Model Matrices

Program, Project & Portfolio Management

	Strategy & Policies	Processes & Controls	People & Organization	Management Reports	Methodologies	Systems & Data
Optimizing	Portfolio alignment strategies frequently evaluated. Portfolio management is agile & supports changing objectives.	PMO processes standardized into all enterprise practices. "Near misses" identified & corrected.	Designated Centers of Excellence support distributed hybrid teams. Standards & training ingrained into operations.	Key PMO metrics continuously balance cost, return, risk and time to allow historical & leading measures.	PMO framework enables continuous portfolio modeling. Portfolio optimization occurs in "real time."	IT demand, program, and project data integrated to allow historical & forward-looking analysis.
Managed	Policy & objectives ingrained into project oversight practices. Service measures designed into process.	PMO processes enforced by effective automated/ preventive controls & monitoring capabilities.	Process/initiative ownership evident throughout enterprise. Training ensures no single points-of-failure.	Management by exception. Analysis of benchmarks used frequently to evolve processes/projects.	PMO framework integrates demand & delivery to develop portfolio balancing scenarios.	Process/project management systems fully integrated. Allow view of demand vs. delivery capabilities.
Defined	Policy & strategy are defined with objectives for project & investment success.	PMO practices widely understood, but may be largely manual. Processes becoming consistently applied.	PMO process ownership is defined. Awareness/training widespread; common PMO oversees some portfolio capabilities.	Key project & portfolio measures (cost, return, time, risk) defined & analyzed regularly.	Portfolio & demand management are integrated into daily operations. Effective use of control "gates" & value measurement.	1-2 primary systems used to manage processes & gather data. Reporting structures defined & readily available.
Repeatable	Basic policy or standard to establish management intent/mission for demand and project management exists.	PMO processes somewhat consistent between groups, but may lack enforced standards tools and/or training.	Multiple PMO functions may exist. Some project/portfolio management exists, but inconsistent execution capability.	Few project/portfolio metrics are defined. Project investment return is assessed by periodic audits and/or manual measurement.	Common project practices defined, but not always followed. Cost/benefit analyses inconsistently applied.	Some automated data collection, but may be redundant or highly manual. Data sources may lack integrity/ integration.
Initial	Project standards and portfolio strategy do not exist or are highly informal.	Project management is reactive, managed informally and very inconsistent across enterprise.	Formal PMO & demand management functions do not exist; responsibility is dispersed.	Only anecdotal evidence available for project, demand and portfolio capabilities.	No overall project methodology exists; siloed/inconsistent processes & standards in use.	Manual/redundant methods used to gather data about projects and overall demand or priorities.

increased Costs

Typical Target Zone

increased Costs

Current Maturity

Partial Demonstration

Target Maturity

Appendix E: Capability Maturity Model Matrices

Security Management

	Strategy & Policies	Processes & Controls	People & Organization	Management Reports	Methodologies	Systems & Data
Optimizing		***N/A – Not Applicable to Most Organizations***				
Managed	Information security strategy aligned with IT/business strategy; Relevant policies in place and adaptable to external conditions and business needs	Standard information security processes emulate and evaluated based on best practice; Risk management integrated with other risk sourcing activities	Centralized security function with highly qualified staff coordinates and enforces objectives; Roles evolve over time with training/technology	Security reporting to management is routing routine, complete, and clear; Performance and risk-based metrics provide an overall view of the organization	Comprehensive security methodology integrates all key components: strategy, policy, risk management, core processes, metrics; Performance improvement continuously identified	A single security dashboard is available to provide real time data from a number of perspectives; Automated data feeds pull from all security processes
Defined	Information security strategy is formally in place and supported by relevant policies; Senior management actively supports security initiatives; Policies are regularly updated	Standard information security processes are documented and consistently performed; Processes are driven by formal risk management which determines resource allocation	Centralized security function with knowledgeable staff coordinates and enforces objectives; Roles defined to ensure accountability across the organization	Management regularly receives reports in a consistent format and is comfortable with the content provided; Key measures are assessed and used to identify risk areas/modify strategy	Comprehensive security methodology integrates most key components: strategy, policy, risk management, core processes, metrics; Performance improvement regularly identified	Processes have been integrated into core security functions to gather business-relevant security data; Automated feeds and processes streamline the process
Repeatable	Core information security policies are documented; policies meet relevant regulatory requirement, but may not be fully enforced	Informal core information security processes are in place; Processes may not be documented, current, or are not systemically enforced	Security roles and responsibilities are in in place; Key individuals have appropriate skills to perform job functions; Training is available and encouraged	Few metrics defined; Metrics are collected regularly but not necessarily in a consistent manner; Metrics typically audit driven	Methodologies are in place for specific security functions which provide a common language; opportunities for improvement identified	Basic and/or manual solutions in place for the collection of data for specific security functions; Data tends to be operational in nature, not risk/value-oriented
Initial	Information security strategies and policies do not exist or are ad hoc in nature; Senior management does not sponsor security initiatives, or is unaware of related security risks.	Core information security processes are not formalized; A formal risk assessment process is not in place to prioritize and address risks and security activities are reactive	Security roles and responsibilities have not been defined to ensure comprehensive coverage and individual accountability; Success relies on individual heroics; training is informal	Reporting on information security functions is informal or does not provide adequate insight into the current state of security	Formal methodologies are not in place to assist with understanding risks and performing security functions; Functions are unpredictable and in a constant state of flux	Limited automated security solutions are in place; Quantitative measures are not integrated into security solutions to allow for value measurement

increased Costs

Typical Target Zone

increased Costs

Current Maturity

Partial Demonstration

Target Maturity

Appendix E: Capability Maturity Model Matrices

Support / Service Desk

	Strategy & Policies	Processes & Controls	People & Organization	Management Reports	Methodologies	Systems & Data
Optimizing	Support is aligned with IT/business strategy; Strategy and process are agile and adapt to changing business needs	Efficient Service Desk function integrates core IT processes; Customer service & advocacy focused; Use "best" practices	Service Desk is knowledgeable, proactive, and enables business; Standards and cross-training are ingrained	Industry leading KPIs; Specified thresholds, targets and effectiveness metrics used to proactively improve performance	Service Desk enables continuous IT improvement; FAQs and known error database are integral to support operations	Technology enables self-diagnosis/ prevention; Tools enable dynamic & static reporting, both historical & predictive
Managed	Policy & objectives ingrained into IT governance practices; Service measures designed into process	Service Desk function established; Incident/ problem integrated with IT processes; Monitoring capabilities exist	Centralized Service Desk closely aligned with other IT functions to prevent issues; Roles, training, and incentives in place	High-quality static, dynamic, and predictive incident/ problem reporting ; KPI trending used to prevent incidents	Centralized Service Desk is single point of contact; Knowledge-base established; High use of KPIs for performance analysis	Extensive use of automation integrated into daily operations; Integration of technologies across all IT processes
Defined	Policy & strategy define objectives for support functions and relationship with business; Formal policy/procedures	Incident/problem formalized and reflect day-to-day practices; Processes are heavily manual, but with some automation	Centralized Service Desk roles well understood by IT/ business; Some cross-training occurs, but mostly informal	KPIs and underlying performance analyzed periodically; Service thresholds in place; Formal reporting techniques are used	Service Desk centralizes incident/ problem processes; IT process integration beginning; Developing FAQs/user guidelines	Stable technology integrates incident/ problem processes; Beginning to integrate with other key IT processes (e.g., CCR)
Repeatable	Basic support policy and strategy exist; Focused on incident response	Incident process focused on reactive resolution; Little problem capability; Process documented but little enforcement	Experienced support staff assigned, but are reactive; Some understanding of responsibilities; Informal training only	Few metrics defined; No process, resource, or satisfaction metrics used; KPIs data may be available, but not used for improvement	Basic Service Desk model to support incident management, but may be used inconsistently.	Minimal automated workflow /escalation automation; Support request management largely manual with individual monitoring
Initial	IT support functions viewed as cost centers only; Policy/ strategy is informal	No standard incident/ problem processes; Only reactive support provided; Processes differ greatly	Call center/help roles may exist, but weakly staffed or siloed; Success due to heroics/staff	KPIs not available; Metric focus on IT spend or downtime; Management is not aware of trends	Weak escalation process in use; No models established; Reliant on people to resolve incidents.	Incident management manual or within inefficient systems; Informal problem management based on "tribal knowledge"

increased Costs

Typical Target Zone

increased Costs

Current Maturity

Partial Demonstration

Target Maturity

Appendix E: Capability Maturity Model Matrices

Governance Practices

	Strategic Alignment	Risk Management	Resource Management	Performance Measurement	Value Delivery
Optimizing	IT is integral to achieving key business strategy objectives. IT proactively identifies and presents solutions to address strategic business challenges.	Risk management is a continuous process coordinated by the Board and senior management. The IT and enterprise level of risk tolerance is widely known.	IT resources are deployed strategically, considering internal and external sourcing models, and are based on defined evaluation criteria linked to business strategies	A balanced scorecard approach is used to continuously monitor IT effectiveness. The scorecard is presented to the Board and other key executives.	IT is viewed as a strategic business partner. Solutions are presented to the business for review, are delivered on time/budget, and achieve the specified scope/objectives.
Managed	The Board and/or executives regularly evaluate alignment between IT and business strategies. Long- and short-term (or tactical) IT plans are mapped to business strategies.	Annual IT risk assessments are completed according to accepted methodologies. Preventative controls and monitoring mechanisms help to validate that key risks are appropriately managed.	IT project, purchasing, asset, and resource management processes are integrated and regularly measured for effectiveness.	IT fully understands the operational performance indicators for the enterprise, and these are regularly measured, monitored, and reported/summarized to IT stakeholders.	IT cost-effectively delivers high-quality services that meet the needs of the enterprise. Communication is frequent and structured. IT proactively seeks to enhance business value.
Defined	A formal process is used to evaluate and prioritize potential IT projects. Established criteria are consistently applied to facilitate cross-functional committee decisions.	IT risks are known, prioritized, and re-evaluated on a regular basis. Mitigation activities are defined for each risk and some monitoring structures are in operation.	IT skill set inventories are maintained and gaps are proactively identified. Formal processes exist to deliver IT personnel and assets to projects and maintenance efforts, as needed.	IT Service Level Agreements (SLAs) with the business are defined and tracked. A formal process exists to review, monitor, and communicate SLA results/ performance.	IT is viewed as an enabler of business processes. There are activities in place to confirm requirements are being met, budget is kept, and goals are being achieved (e.g., ROI).
Repeatable	IT maintains existing systems but is viewed primarily as an order taker by the business units. Project decisions involve business personnel and require business cases.	IT risks have been identified and are being tracked with some mitigation activities in place. IT adequately responds when an incident occurs, but procedures are informal.	An organization-wide organization chart exists and is maintained. A list of applications and infrastructure assets can be generated, but it may not be reliable or current.	Some measures are regularly assessed across IT and are consistently communicated. There are gaps between what is measured by IT and what the business would like to have measured.	IT is viewed as a consistent utility provider. IT-business communication is fairly consistent, but interaction is typically issues-focused. There is little formal analysis of goal achievement.
Initial	IT projects and services may inconsistently align with business needs/objectives. Project decisions are made unilaterally or without established criteria.	IT lacks understanding of the risks that may exist across the entire company landscape. Risk assessment activities occur occasionally or in response to an incident.	IT reporting lines and skill sets are known by management, but they are not inventoried or organized. IT asset management is informal.	Some measures are assessed within a few IT areas. Results may be informally communicated and data are not used to source or proactively address issues.	Communications between IT and the business are irregular and/or ineffective. Projects are often delayed; do not deliver specified scope, and/or are over budget.

increased Costs

Typical Target Zone

increased Costs

Current Maturity

Partial Demonstration

Target Maturity

Powerful Insights.
Proven Delivery.™

Confidentiality Statement and Restriction for Use

This document contains confidential material proprietary to Protiviti Inc. ("Protiviti"), a wholly-owned subsidiary of Robert Half International Inc. ("RHI"). RHI is a publicly-traded company and as such, the materials, information, ideas, and concepts contained herein are non-public, should be used solely and exclusively to evaluate the capabilities of Protiviti to provide assistance to your Company, and should not be used in any inappropriate manner or in violation of applicable securities laws. The contents are intended for the use of your Company and may not be distributed to third parties.

protiviti®