Enterprise Risk Management (ERM) Project

Information and Communications Technology

Summary Report to the Audit Committee

December 6, 2011

Prepared and Presented:

Jeff Hollingsworth

Lauren Smith

1. **Process Overview**
   - Overview of ERM ICT Project and Key Activities Completed
   - 17 Risks Selected for Discussion, Assessment and Prioritization

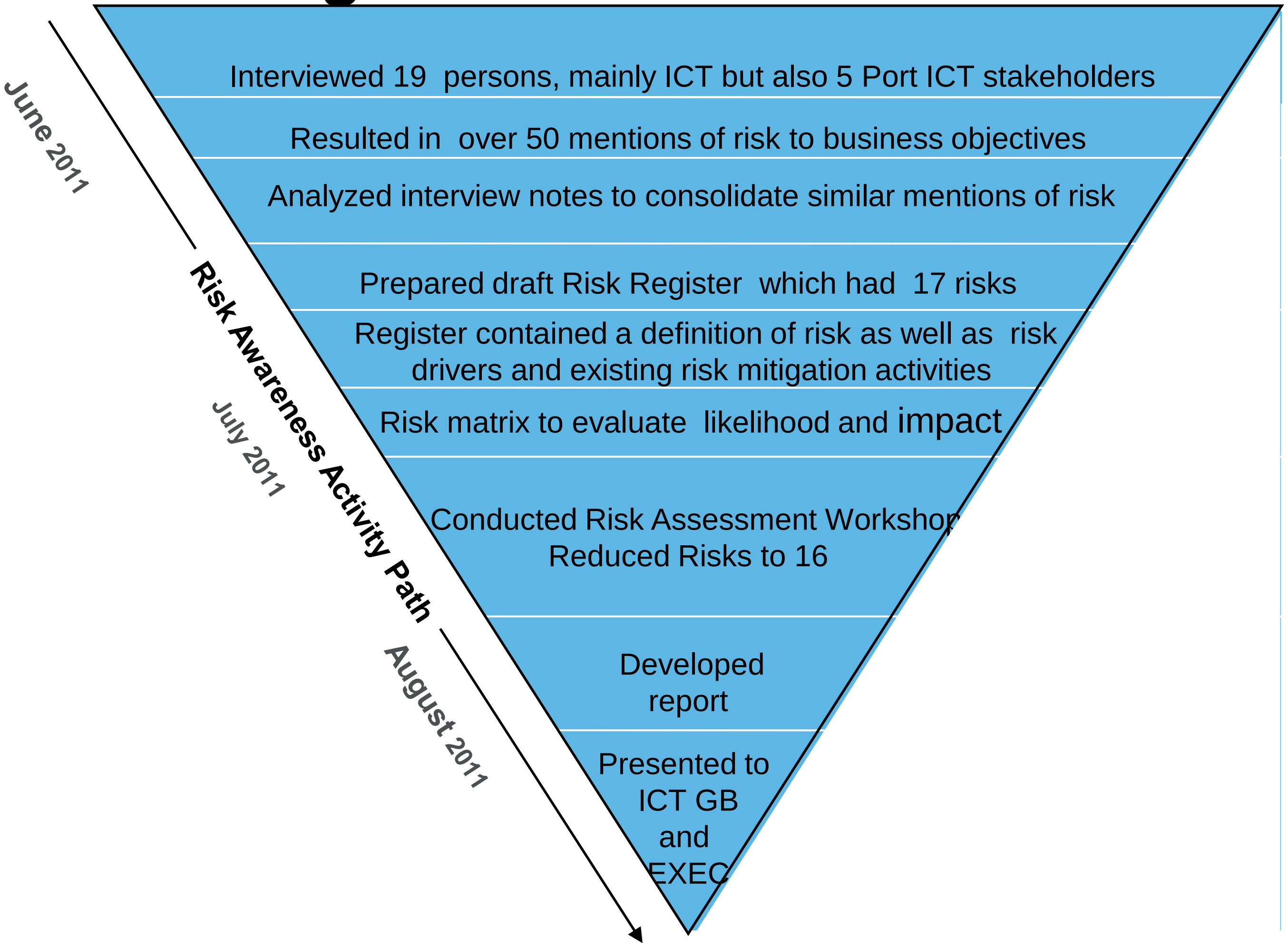
2. **Communication of Results**

3. **Risk Assessment & Prioritization Workshop Results**
   - Risk Ranking Process
   - Risks Prioritized According to Risk Ranking
   - ICT Services Enterprise Risk Map
   - Detailed Risk Overviews
   - Risk Action Planning
   - Risk Matrix for Impact and Likelihood

4. **Discussion of Next Steps for ICT**

5. **Discussion Items for Port on ERM**

Focusing on the Most Critical Risks



Interviewed 19 persons, mainly ICT but also 5 Port ICT stakeholders

Resulted in over 50 mentions of risk to business objectives

Analyzed interview notes to consolidate similar mentions of risk

Prepared draft Risk Register which had 17 risks

Register contained a definition of risk as well as risk drivers and existing risk mitigation activities

Risk matrix to evaluate likelihood and impact

Conducted Risk Assessment Workshop
Reduced Risks to 16

Developed report

Presented to ICT GB and EXEC

Risk Assessment & Prioritization Workshop Results

Information and Communications Technology - Risks For Assessment

#	Risk Name
1	Change Management
2	Complexity and Volume of Systems
3	Contracting
4	Employee Engagement
5	Financial Model
6	ICT Budget
7	ICT Business Model
8	ICT Department Leadership
9	Internal Processes
10	Decentralized Systems

#	Risk Name
11	Leadership
12	Natural or Manmade Disasters
13	Roles and Responsibilities
14	Security and Compliance
15	Staffing
16	Technology Marketplace
17	Workload
18	
19	
20	

Workshop participants assessed each risk on two criteria:

- The estimated likelihood of a risk’s occurrence
- The estimated impact of a risk’s occurrence on ICT’s ability to meet its strategic objectives

The assessments of Impact and Likelihood are used to develop Risk Maps to focus management attention on the most critical risk risks.

RISK ASSESSMENT WORKSHEET

INFORMATION AND COMMUNICATIONS TECHNOLOGY

Port of Seattle

Score	LIKELIHOOD			IMPACT					
	Measure	Description		Description	Financial (US$)	Operational	Compliance/Security	Community	Employees
9	**ALMOST CERTAIN** Something already happening on a regular basis.	Almost Certain		Critical	**CRITICAL** Additional expenses in excess of 20% of approved budget	**CRITICAL** Mission critical systems down in excess of four hours and/or 25% of Port staff unable to do their jobs due to unavailability of technology resources and/or loss of critical data.	**CRITICAL** Multiple incidents of non-compliance with security (PCI) and/or findings by Internal Audit department, State Auditor and/or Federal Investigators of serious violations with clear indications of breach of protected data, non-compliance with PCI, and fraud and/or fines imposed on Port and/or legal judgments imposed against Port and/or shut down of credit card processing and/or cash transfer functions.	**CRITICAL** Sustained (e.g., longer than three days), multi-media negative international and national media coverage (i.e., top/front page story); Multiple parties or groups represented at public protests and/or comments made during multiple Commission meetings.	**CRITICAL** Loss of or lack of availability of key staff and/or skill sets in mission critical systems and/or extensive period of time with key ICT positions not filled.
7 to 8	**LIKELY** Something already happening on a regular basis but overall temporary in nature.	Likely		Major					
5 to 6	**POSSIBLE** Something not happening currently, but anticipated to happen.	Possible		Moderate					
3 to 4	**UNLIKELY** Something not happening but it could in very infrequent cycles.	Unlikely		Minor					
1 to 2	**RARE** Something not happening and not anticipated to happen.	Rare		Insignificant	**INSIGNIFICANT** No unbudgeted expense	**INSIGNIFICANT** Minimal or no downtime for mission critical systems	**INSIGNIFICANT** No compliance concerns reported from any channels; no evidence to support lack of compliance; No fines or legal judgments against the Port.	**INSIGNIFICANT** No media coverage; No public comments at a Commission meeting.	**INSIGNIFICANT** No loss of staff or skill sets. No impact or delays in filling key ICT positions.

Information and Communications Technology – Example of Risk Definition:
Complexity and Volume of Systems

Risk Definition

COMPLEXITY AND VOLUME OF SYSTEMS: Risk that the many applications at the Port create a drain on resources that dilutes attention or focus on more critical projects.

Risk Drivers

- Linking organizational assets to applications
- Linkages between systems increases complexity
- Multiple versions of same application in use throughout the org.
- Vendor provided solutions sometimes increase complexity
- Potential for system failure
- Staggered timeline of application life cycle overlaid on business needs and evolution of technology
- Address ICT issues from internal global perspective rather than department/user specific perspective (e.g., what's best for the Port vs. what's best for Dept X)
- Actually 2000+ separate applications/versions in use at the Port
- Impacts approach we take to tech investments we make at the Port

Existing Risk Management Activities

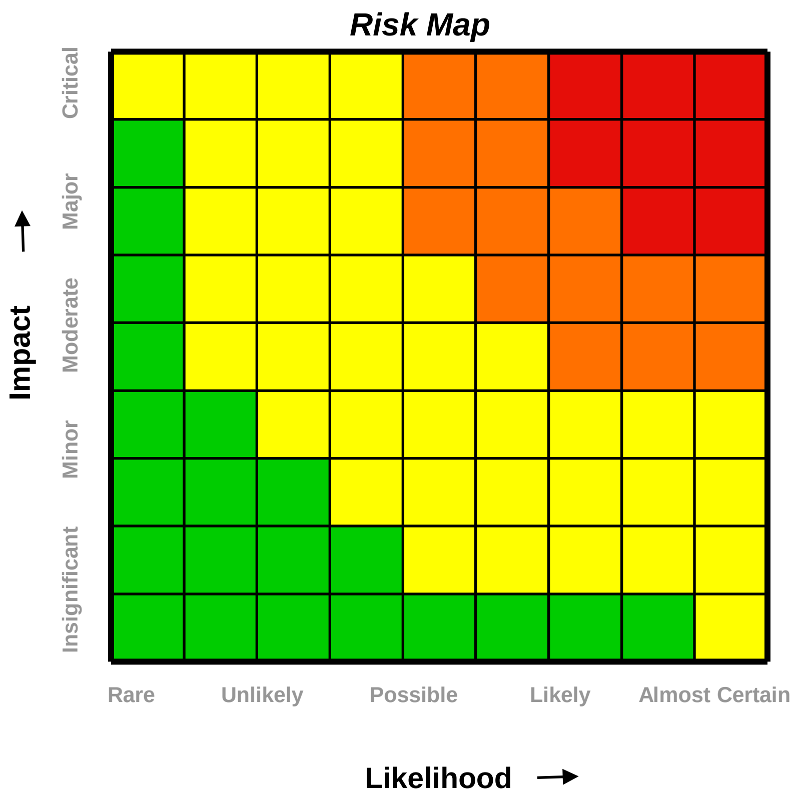
- Want to standardize network gear
- Architecture board
- Managed at more senior level
- Tracking hardware warranties, lifespan of operating systems, application lifecycles.
- Shifting from local admin access to user level access

Risk Assessment & Prioritization Workshop Results

Information and Communications Technology - Risk Ranking Process

Initial Prioritization Based Upon Assessments of Impact and Likelihood

Risk Ranking Matrix



Risk Ranking Overview

- Risk Ranking provides an initial means of prioritizing assessed risks based upon assessments of Impact and Likelihood
- Risk Rankings are used to identify a risk's position on a Risk Map (see chart to left)

Risk Ranking Calculation Steps

- Multiply the Impact assessment (on a scale of 1-9 with 9 being the highest impact and 1 being the lowest) and the Likelihood assessment (on a scale of 1-9 with 9 being the highest likelihood and 1 being the lowest) for each risk
- Reference the product against a range of values (see table below)

Risk Rankings

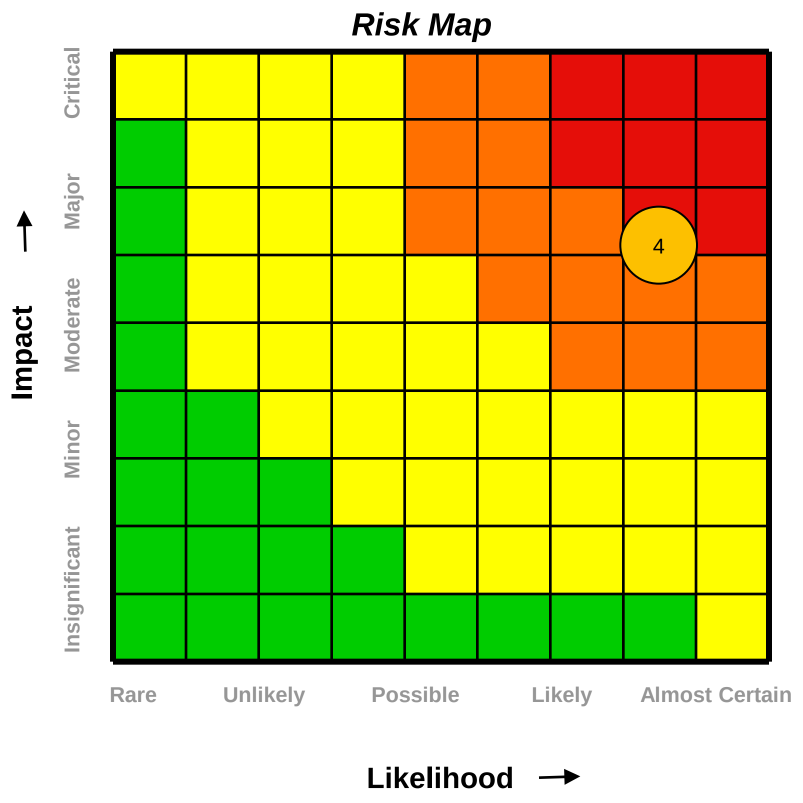
Risk is ranked as…	*…if the product of Impact & Likelihood is…*
VERY HIGH	Greater than ***49.0***
HIGH	Greater than ***27.0***, but less than ***49.0***
MEDIUM	Greater than ***9.0***, but less than ***27.0***
LOW	Less than ***9.0***

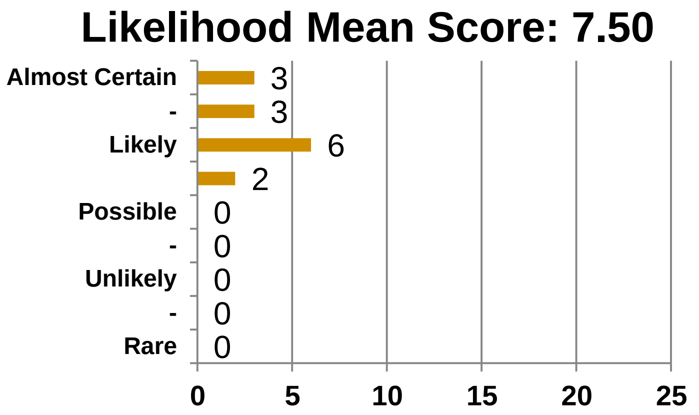
Information and Communications Technology - Detailed Risk Overview

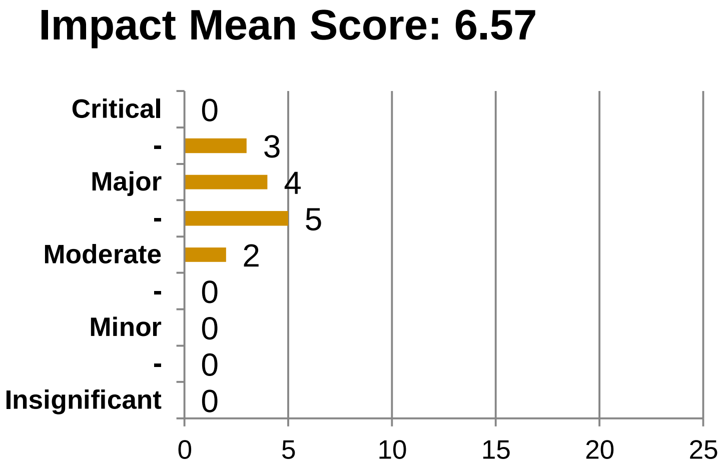
Complexity and Volume of Systems

COMPLEXITY AND VOLUME OF SYSTEMS: Risk that the many applications at the Port create a drain on resources that dilutes attention or focus on more critical projects.

Risk Score = 49.28







Risk Assessment & Prioritization Workshop Results

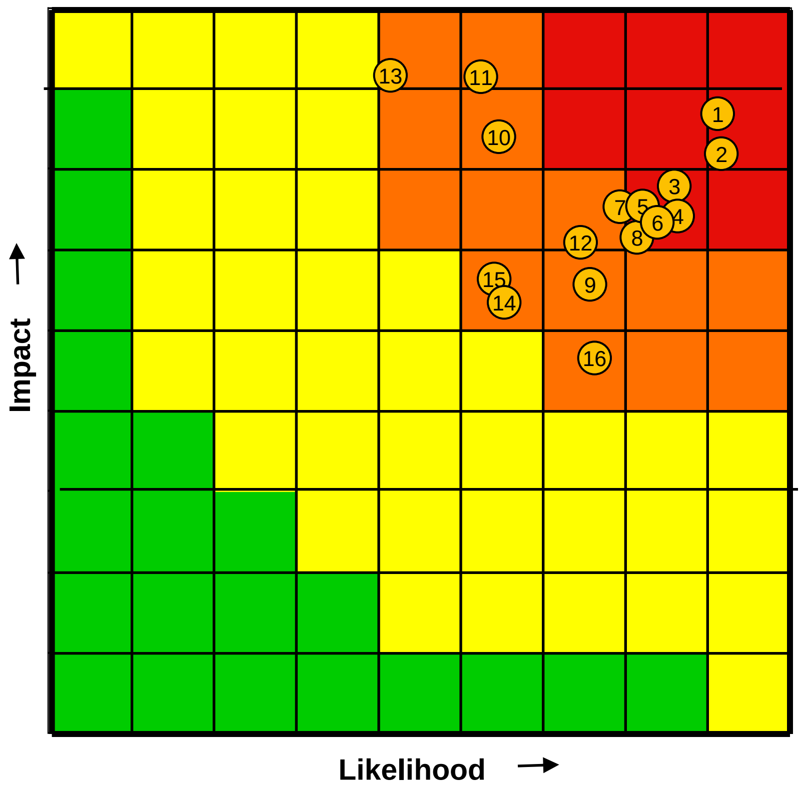
Information and Communications Technology -Risks Prioritized to Risk Ranking

Rank	Risk Name	Likelihood	Impact	Risk Ranking
1	Decentralized Systems	8.38	7.85	**65.78**
2	Internal Port Processes	8.46	7.46	**63.11**
3	ICT Budget	7.23	6.92	**50.03**
4	Complexity and Volume of Systems	7.50	6.57	**49.28**
5	Leadership	7.15	6.77	48.41
6	Roles and Responsibilities	7.49	6.46	48.19
7	Contracting	7.00	6.79	47.53
8	Change Management/Employee Engagement	7.21	6.07	43.76
9	Staffing	6.54	6.62	43.29
10	Compliance	5.54	7.46	41.33
11	Security	5.07	8.07	40.91
12	Workload	6.54	6.08	39.76
13	Natural or Manmade Disasters	4.23	8.00	33.84
14	Enterprise Technology Strategy	5.71	5.71	32.60
15	ICT Department Leadership	5.54	5.77	31.97
16	Technology Marketplace	6.85	4.54	31.10

Risk Assessment & Prioritization Workshop Results

Information and Communications Technology Enterprise Risk Map

ICT Enterprise Risk Map



Rank	Risk Name	Risk Ranking
1	Decentralized Systems	65.78
2	Internal Port Processes	63.11
3	ICT Budget	50.03
4	Complexity and Volume of Systems	49.28
5	Leadership	48.41
6	Roles and Responsibilities	48.19
7	Contracting	47.53
8	Change Management/Employee Engagement	43.76
9	Staffing	43.29
10	Compliance	41.33
11	Security	40.91
12	Workload	39.76
13	Natural or Manmade Disasters	33.84
14	Enterprise Technology Strategy	32.60
15	ICT Department Leadership	31.97
16	Technology Marketplace	31.10

Possible Next Steps for ICT Consideration

- Assess current mitigation efforts for identified risks or top priority risks
  - Identify which risks are good targets for risk mitigation potential.
  - Evaluate current mitigation efforts.
  - Ask whether mitigation is aligned with risk tolerance thresholds?
  - Determine any budget impacts for risk mitigation

- For priority risks - create integrated risk mitigation plans
- Identify sponsor and set timeline

- Implement mitigation and monitor results

Items General Port Discussion

- **Where does Port take ERM moving forward and what do we do with ERM results?**
  - ERM assessment versus performance audit
  - Response to findings
  - Mitigation efforts – funding for

- **Who is the audience for reporting ERM findings?**
  - Audit Committee versus Commission or both
  - Division finance and budget

- **Establish Roles & Responsibilities and Policies & Procedures**
  - What is the merit of establishing an ERM process and identify ERM roles and responsibilities

- **Establish Initial Risk Reporting Framework**
  - Should formal reporting tools and approaches for ERM results be created?

- **Define Risk Appetite and Tolerances – Recommendation from Last Year's Consultants**
  - Formally define the Port's risk appetite and establish a consistent and documented approach to understanding risk drivers, risk management options, and governance for key risks

Appendix
ICT ERM Project Participants

The Port of Seattle representatives who participated in the ICT ERM Project are listed below .

Peter Garlock, Chief Information Officer*	Matt Breed, Sr. Manager ICT Infrastructure Services
Kim Albert, Senior Manager, IT Business Services*	Krista Sadler, Manager ICT Project Management
Dave Wilson, Chief Technology Officer	Brad Jensen, Mgr Security & Pub Safety Tech Information Technology
Tony Butler, Senior Manager of Service Delivery*	Ed Goodman, Development QA Mgr/Sr. Software IT
Lindsay Pulsifer, Manager of Marine Maintenance	Mark Coates, Senior Manager Operations – Airfield Operations
Paul Cocus, Manager of ICT Client Services and Support*	Rudy Caluza, Director of Accounting and Procurement
Dakota Chamberlain, Seaport Project Manager	Lindsay Pulsifer, General Mgr. Seaport Maintenance
Devron Knowles, Sr. Network Engineer	Harold Federow, ICT Contract Manager and IP Manager
Paul Jeyasingh, Systems Engineering Manager	Jim Dawson, Manager of Windows Server Engineering
Mike Ehl, Director of Airport Operations	Mary Gardner, Manager of ICT Disaster Recovery