

Risk Management

Risk at Small and Medium-Size Ports

June 2024
V1.1

U.S. Department of Homeland Security
United States Coast Guard

U.S. Coast Guard
International Port Security Program

Collaborative Risk Management Pillar

Goal

Strengthen the economic viability of international ports and their role supporting the global economy by applying a layered approach to the Port Facility Security Plan (PFSP), collaborating with port stakeholders, building an organizational structure based in interagency cooperation, and improving risk communications.

Themes

Collaborative Risk Management	Systemic Management of Port Security	Effective Management of Port Security Operations
"Managing Risk is Good for Business"	*"Security is Everyone's Business"*	*"Security is Good for Business"*

Modules

• Risk Management • Continuous Improvement • Evolving Maritime Security Threats • ISPS Code Review • Cyber Security	• Collaborative Approach • Stakeholder Management • Committees	• Dynamic Environments • Implementing • Planning / Organization • Staffing / Training • Leading

Agenda

- Identifying Risks (Collaborating with key agencies)
- Risk Assessments (Regional and National level)
- Risk Management (Policy, Procedures & Techniques available to counter the threats)



Identifying Risks

Discussion

Discuss the following questions:



- How would you define risk?
- Do you consider risk to be positive, negative, or both? Why?
- What decisions / tasks often involve high or low levels of risk?

What is Risk?

Risk can be defined in many ways but encompasses two main components.

- The possibility of danger
- Its potential consequences

Risk can be positive, negative, or both.



Four Risk Quadrants



Types of Risk in Each Quadrant

Hazard
- Cybersecurity
- Environmental concerns
- Employee injuries



Operational
- Employment practices
- Regulatory compliance
- Critical equipment losses

Financial
- Economic instability
- Recession
- Budget overruns

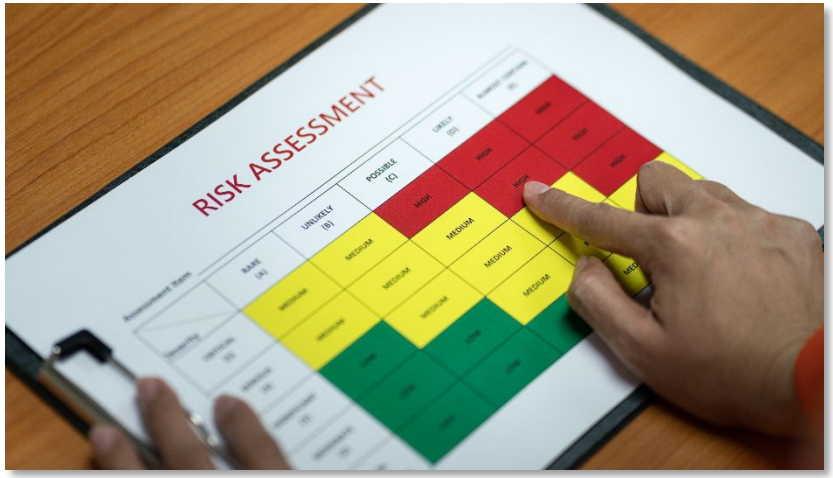
Strategic
- Reputation
- Information technology
- Political environment



Risk Assessments

What is a Risk Assessment?

- Risk assessments determine the degree of exposure to hazards or dangers to personnel and property.
- Risk assessments are a step in identifying measures to minimize risk.
- Risk assessment processes vary by the organization's needs.



Risk Assessment Considerations

Assets

- People, property, business process, or function

Consequences

- The effects or outcomes
- Often ranked: Low, medium, or high

Criticality

- The consequence of failure
- Assigned a value to determine most important

Threats

- Consistent with the Port Facility Security Assessment and Port Facility Security Plan

Vulnerabilities

- Flaw or weakness that could be exploited
  - Accessibility, availability, facility, and security

Technique: Threat and Risk Assessment Matrix

Potential Target (PT): _____

Scenario No.	Threat Scenario	Threat Odds	Vulnerability of Existing Measures	Impact	Risk Score	Action Priority
Assign a number	Describe the scenario	3: High 2: Med 1: Low	4: None 3: Minimal 2: Acceptable 1: Effective	5: Security / Safety 4: Public Safety / National Prestige 3: Environment / Economic 2: Assets / Infrastructure 1: Customer / Reputation	C x D x E = F	#

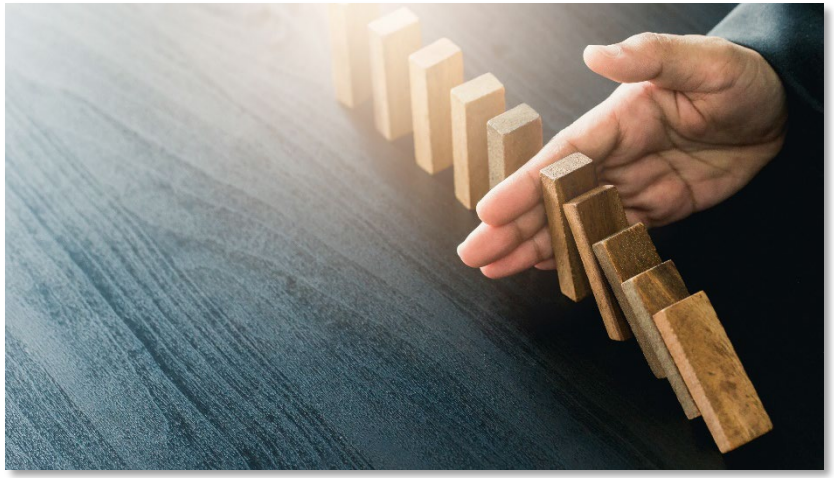


Risk Management

What is Risk Management?

Risk management uses coordinated activities to direct and control an organization's acceptable level of risk.

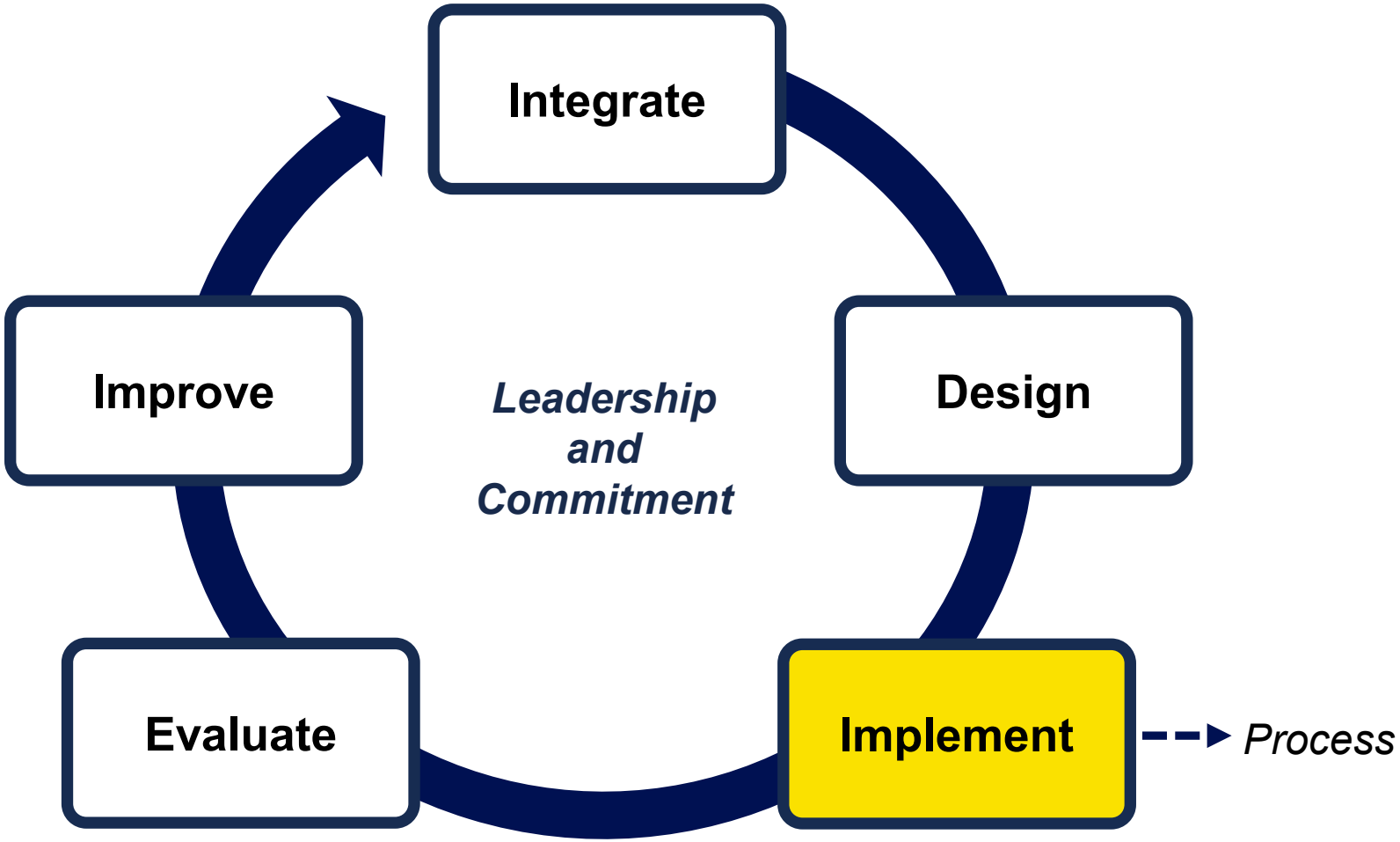
- Coordinated activities are structured through both a framework and process.



Dynamic Environment Impacts

- Post 9/11, risk management occurs in a national security environment.
  - Increased need for collaboration between port users, stakeholders, and public and private partnerships.
- Generating buy-in from the port community is essential to efficient port security management.
  - Resolve conflicted interests
  - Seek the cooperation of port users in risk assessment process
- *PFSP must be based on assessment models that are rational, balancing efficiency with effectiveness.*

Risk Management Framework



Risk Management Techniques / Strategies

Acceptance

- Accepting the consequence without trying to change probability or impact

Avoidance

- Never beginning an activity / possibility of future loss is eliminated

Loss Prevention

- Reduces the frequency of a particular loss

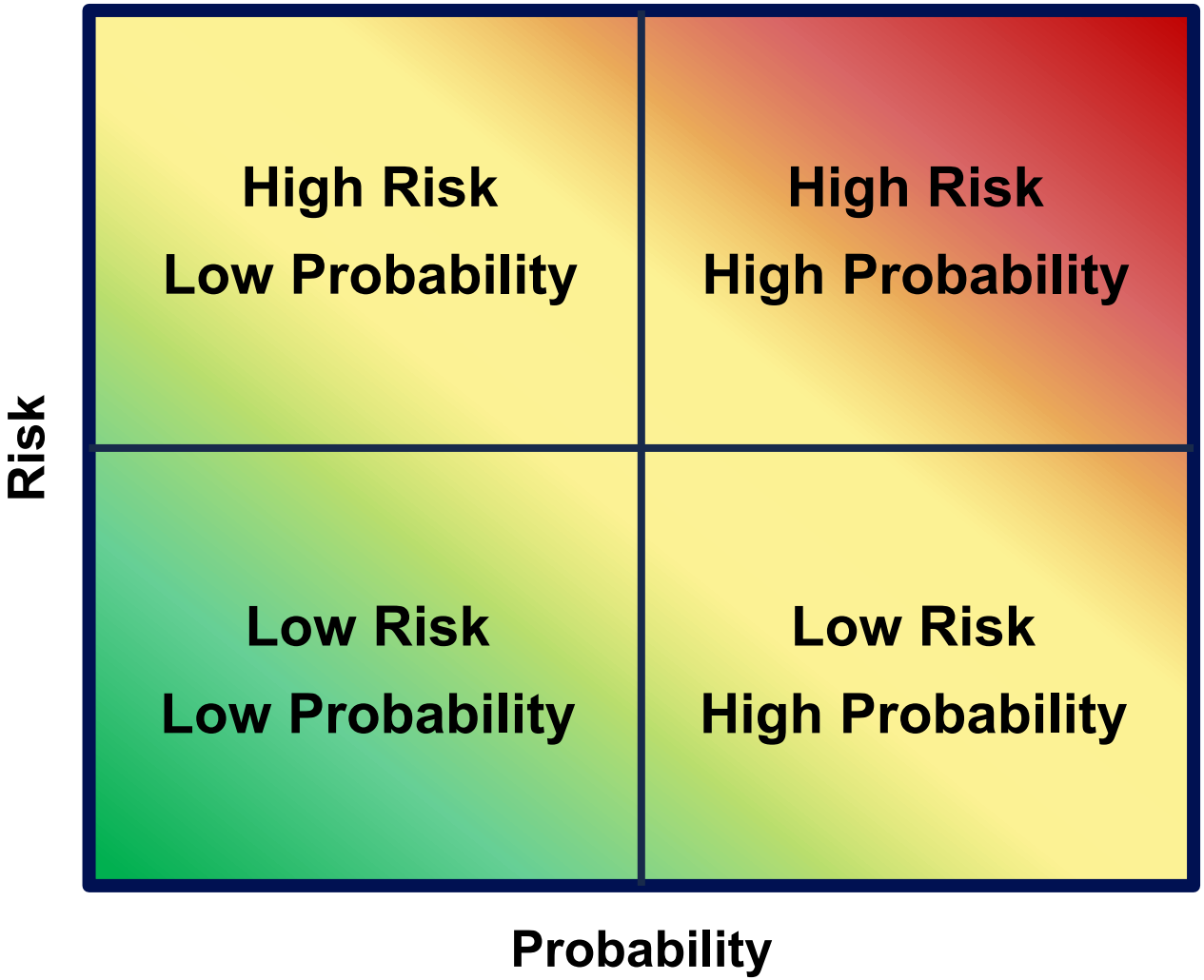
Loss Reduction

- Reduces the severity of a particular loss
  - Disaster recover plan – specialized aspect of loss reduction

Transfer

- Assigning the ownership or liability of the risk to another party

Risk Matrix


High Risk
Low Probability
High Risk
High Probability
Low Risk
Low Probability
Low Risk
High Probability
Risk
Probability

Dynamic Environment Impacts

- Risk management for medium-sized ports in the Caribbean focuses on a mix of severe climate events, operational congestion, physical and maritime security, and emerging digital threats.

  - Natural Hazards & Severe Weather Systems (e.g. Hurricanes)

  - Operational & Navigational Risks: Rising trade volumes, larger vessel classes, *and growing cruise calls increase congestion*, collision risks, and pollution pressures in MARPOL-designated sensitive marine zones

  - Cybersecurity Threats: The adoption of digital tools like Port Community Systems (PCS) and mobile management apps exposes medium-sized ports to ransomware, phishing, and operational disruption

Dynamic Environment Impacts

- The most effective risk management techniques for port facilities are structured below across five operational pillars:

1. Technology-Driven Screening (Non-Intrusive Inspection)
2. Eliminating the "*Insider Threat*"
3. Smart Container Integrity Programs
4. Port Intelligence Partnerships
5. Upgrading Physical and Perimeter Defenses

Dynamic Environment Impacts

1. Technology-Driven Screening (Non-Intrusive Inspection)
   - High-Throughput NII Systems: Deploying drive-through X-ray and Gamma-ray portal scanners allows ports to scan
   - Digital profile of the cargo without opening the doors.

2. The greatest vulnerability in any medium-sized port is not the perimeter fence.
   - Subverted employee
   - Strict personnel controls
   - Biometric Access & Segmented Zoning
   - Continuous Vetting & Randomization
   - Dual-Authorization Protocols

Dynamic Environment Impacts

3. Smart Container Integrity Programs

   Managing "Rip-on/Rip-off" smuggling risks, ports must secure the physical container asset

   a. E-Seals and RFID Tracking
   b. Mandate use of Electronic Seals (E-Seals)
   c. Enforced "Sterile Zones“

4. Port Intelligence Partnerships

5. Upgrading Physical and Perimeter Defenses

Dynamic Environment Impacts

- Managing the *insider threat* in Caribbean ports requires moving away from the assumptions that all employees inherently are trustworthy.
  - Shifting to a *"Zero-Trust" Security Model*.

- Most effective management techniques for mitigating insider threats are structured in five operational layers:

1. Segregated Physical Access Control (Micro-Zoning)
2. Eliminating Single-Point-of-Failure (The Dual-Authorization Rule)
3. *Mitigating Data and Manifest Tampering*
4. *Continuous Vetting and Institutional Integrity*
5. Rigorous Sterile Zone Management

Dynamic Environment Impacts

1. Segregated Physical Access Control (Micro-Zoning)

1. Eliminating Single-Point-of-Failure (The Dual-Authorization Rule)

2. Mitigating Data and Manifest Tampering

3. Continuous Vetting and Institutional Integrity

4. Rigorous Sterile Zone Management

Dynamic Environment Impacts

- Managing the *Cyber threat* in Caribbean ports requires:
  - Establishing a Cybersecurity Framework (CSF)
  - National Institute of Standards and Technology (NIST from US Department of Commerce)
  - CSF can assist in managing and reduce their cybersecurity risks and improve cybersecurity program already in place.

- The CSF 2.0 is organized by six Functions:
  - **Govern, Identify, Protect, Detect, Respond, and Recover.**

Dynamic Environment Impacts

GOVERN : The organization's cybersecurity risk management strategy, expectations, and policy are established, communicated, and monitored.

IDENTIFY : The organization's current cybersecurity risks are understood.

PROTECT: Safeguards to manage the organization's cybersecurity risks are used.

DETECT: Possible cybersecurity attacks and compromises are found and analyzed.

Dynamic Environment Impacts

RESPOND: Actions regarding a detected cybersecurity incident are taken.

RECOVER: Assets and operations affected by a cybersecurity incident are restored.



Questions?

Risk Management for Small and Medium Sized Ports (Caribbean region)