

Charting a Course to Energy Independence

**Providence, RI
August 9-12, 2009**





Evolving Energy Environment

- ▶ Falling off of new oil finds (Peak Oil)
- ▶ Supply threats (vulnerabilities in the supply chain)
- ▶ Increased demand for energy in the developing world
- ▶ Push for greater energy efficiency and use of alternative energy sources
- ▶ Growing role of IT in distribution (ex. Smart Grid)
- ▶ Increasing capabilities/will of nation states/non-state actors/individuals to disrupt distribution systems
- ▶ Carbon foot print



Strategic Risk Management (SRM)

Table of Contents

Value Drivers

SRM Methodology

Sample SRM Case Study



Organizations tend to have similar challenges and needs in focusing on mission execution

Common Challenges

- ▶ Limited Resources
- ▶ Allocation of funding
- ▶ Time constraints
- ▶ Ever-changing functional processes
- ▶ Limited coordination between divisions

Common Questions

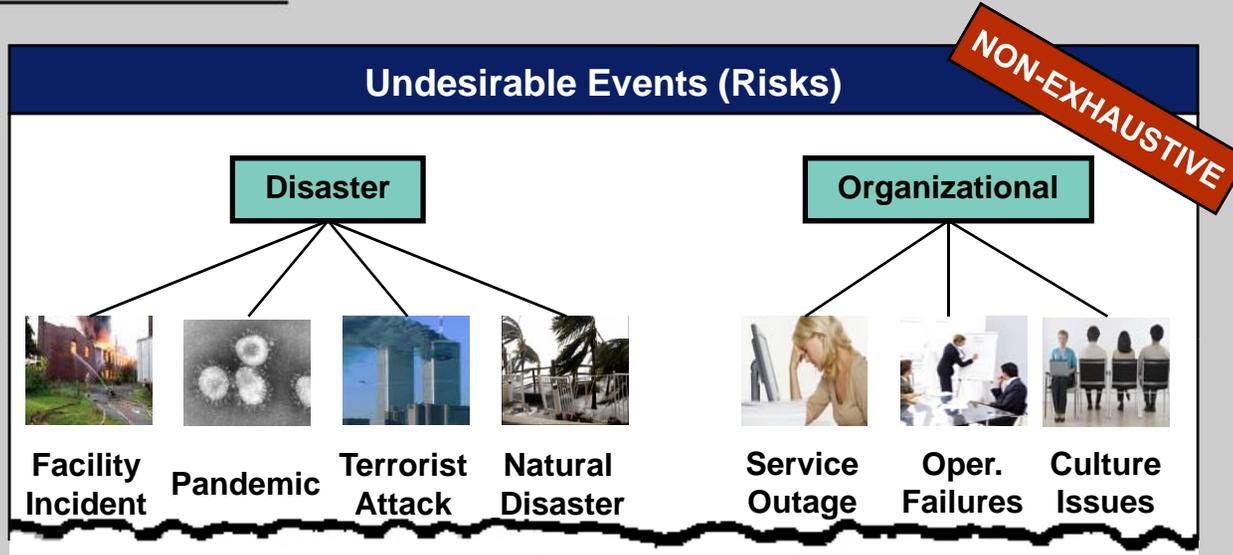
- ▶ What are the key risks to my business / mission?
- ▶ How effectively can we mitigate or capitalize on those risks?

Common Needs

- ▶ Tool for allocation of resources
- ▶ Justification for funding distributions
- ▶ An enterprise focus on threats to the organization
- ▶ A safe forum for communication between functional leaders
- ▶ Shared view of how to pursue mission execution



Growing visibility and emphasis on both preparedness and justifying resource allocation is increasing interest in risk management



After an undesirable event, can an organization justify their preparations and response?

- ▶ Do you have a structured risk management program in place?
- ▶ Does your approach meet the evolving definition of a good “control environment”?
- ▶ Is risk management integrated into your budget decision making?
- ▶ Why didn't we allocate more funds to mitigate against this risk?
- ▶ Who approved the decision to accept the risk of the undesirable event?
- ▶ Can you account for all roles and responsibilities during this crisis?

Business Consequences

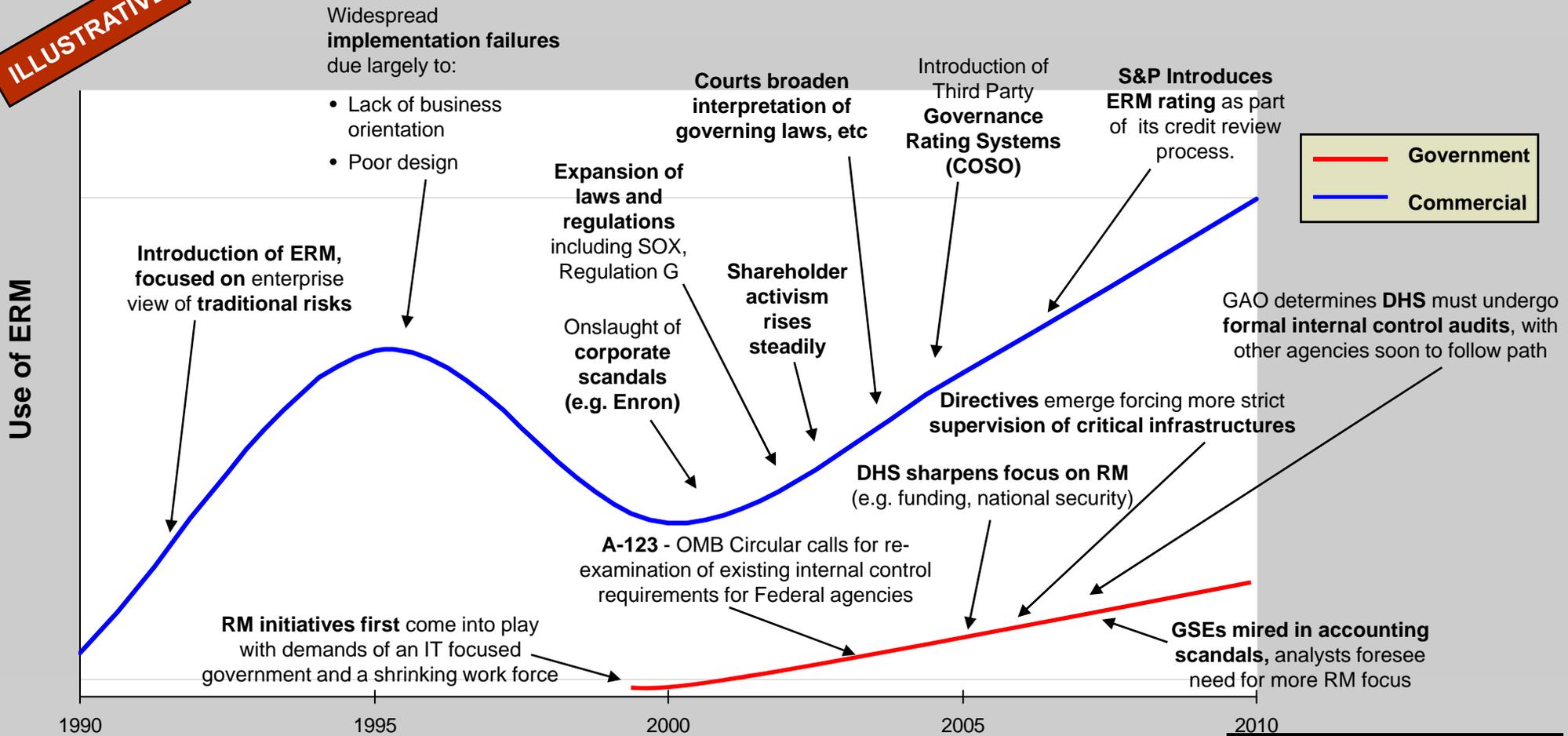
- ▶ Investigations (e.g., OIG, legislative, media)
- ▶ Undesirable publicity
- ▶ Deteriorating operating performance
- ▶ Legal exposure
- ▶ Declining confidence of customers
- ▶ Adverse employee relations



Booz Allen developed Strategic Risk Management (SRM) to drive the commercial ERM wave, and has applied lessons learned to burgeoning government markets

ILLUSTRATIVE

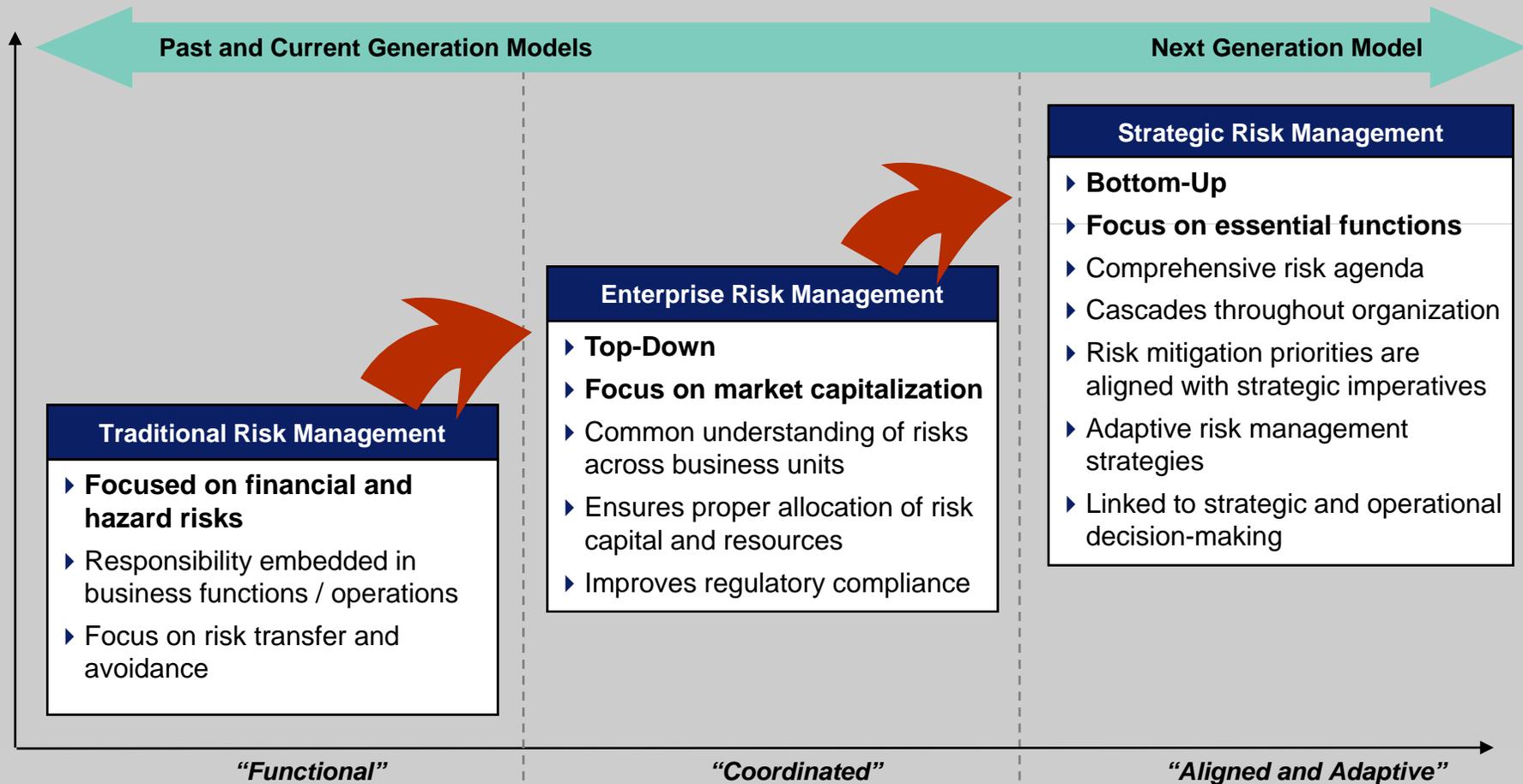
Adoption of ERM





SRM is the evolution beyond a functionally “siloed” view of risk management to an integrated, adaptive approach

Risk Management Maturity Model



Source: Booz Allen benchmarking studies and analysis



Strategic Risk Management (SRM)

SRM Table of Contents

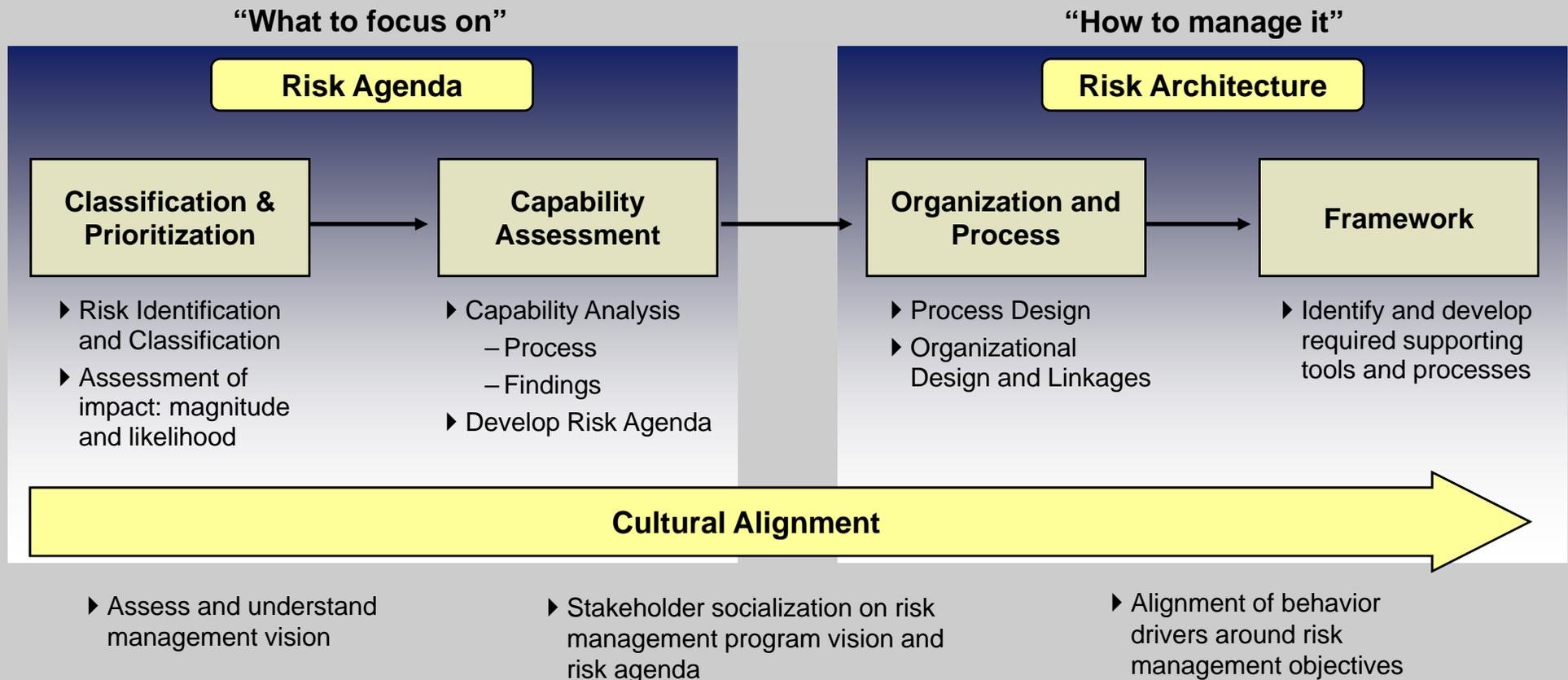
Value Drivers

SRM Methodology

Sample SRM Case Study



A robust risk management program has three primary elements – the agenda, the architecture, and the underlying cultural alignment





SRM is a four-step framework to identify, address, and manage the strategic risks facing an organization

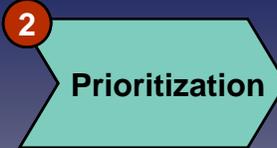
Agenda



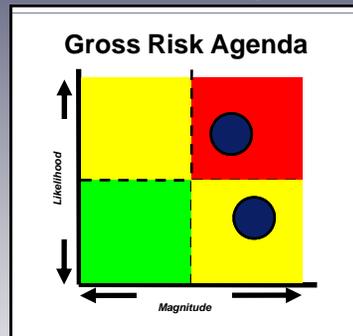
Risk List

1	Targeted Messaging attacks (e.g. Phishing, P2P, Instant Messaging) on internal systems allow secretive command-and-control by a botnet
2	Close proximity transmission intercepts (e.g. via Blackberry, laptop, wireless access point) permit intrusion into core LAN infrastructure
3	Increasingly sophisticated malicious code embedded in Web 2.0 websites allows system exploitation opportunities
4	Mission essential IT systems that use COTS-based software introduce publicly available security vulnerabilities
5	Compromised hardware / software introduced into local environment due to adversaries involved in the supply chain process

- ▶ Comprehensive, wide-aperture risk list
- ▶ Risks that are not identified by traditional risk management



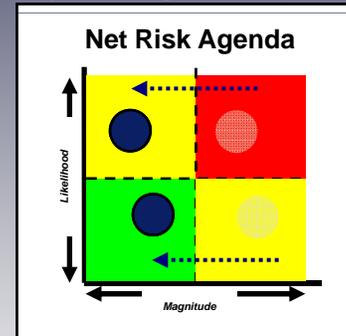
Prioritized Risk Agenda



- ▶ “Gross” prioritization of largest risks facing an organization



Analyzed Mitigation Capabilities



- ▶ “Net” prioritization of largest risks with least current ability to mitigate
- ▶ Deep understanding of risks after factoring in mitigating capabilities

Architecture



Actionable Steps

Prioritized List of Capabilities that Buy-Down the Most Risk

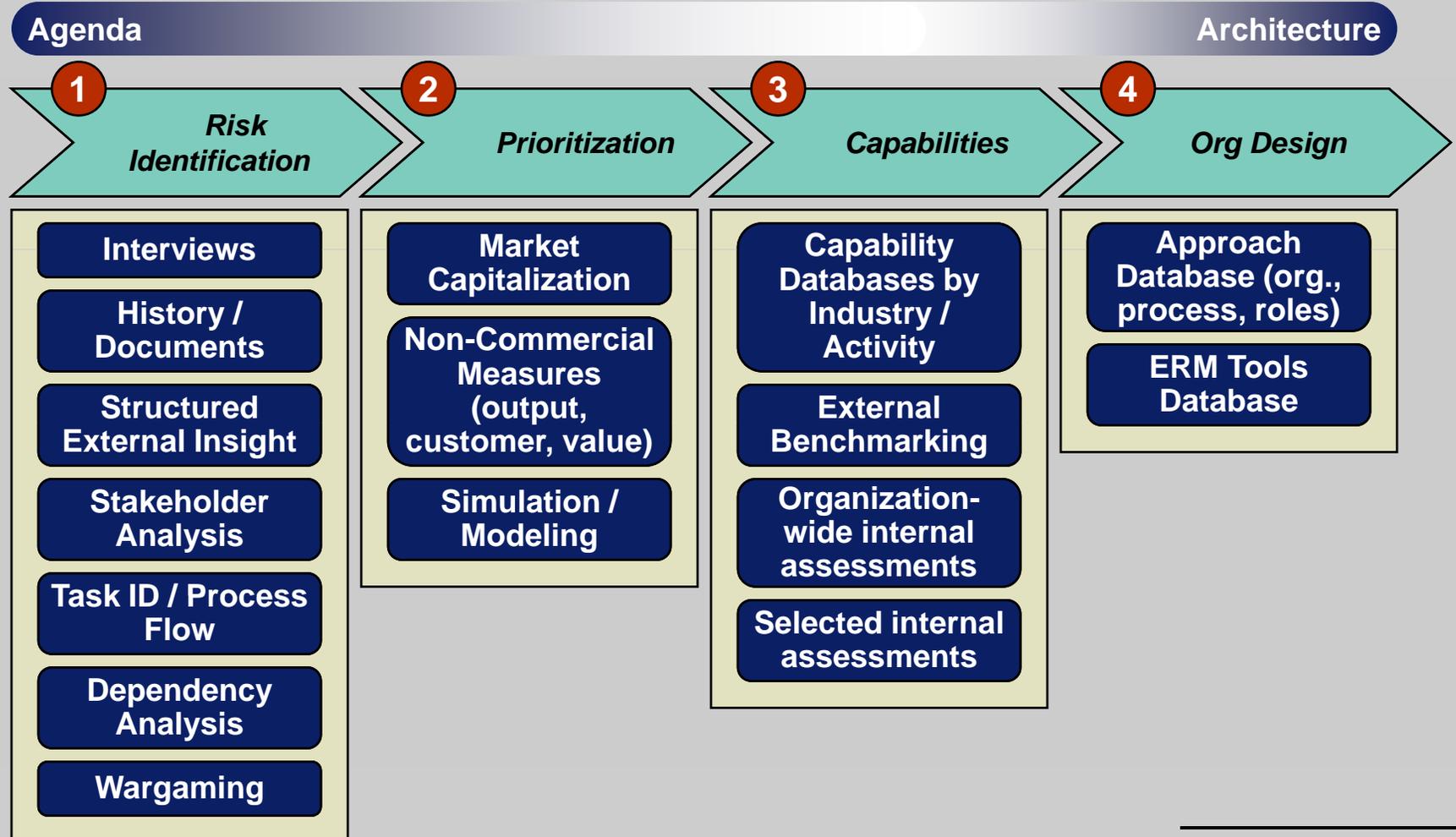
1	Procurement Efficiency
2	IT Customer Support
3	Technology Insertion
4	Workstation Strategy

- ▶ Sustainable risk management benefits
- ▶ Increasing maturity towards a “risk-based” culture



Specific methodologies chosen within each step are dependent upon the client's specific situation, challenges, and objectives

Booz Allen SRM Methodologies





Strategic Risk Management (SRM)

SRM Table of Contents

Value Drivers

SRM Methodology

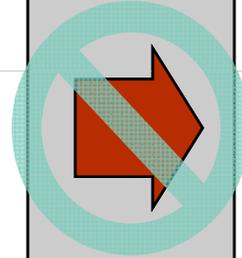
Sample SRM Case Study



SRM can enable functional managers to effectively address risks outside of their scope, authority, or resources...

Functional Risk Management Challenges

- ▶ BU management is tasked with functions that face BU-specific risks / obstacles and has developed BU-specific capabilities to overcome them
- ▶ However, many BU-specific capabilities are dependent upon the effective functioning of other BU capabilities and the organization's ability (or inability) to address the major risks to the enterprise
- ▶ Functional managers often lack the senior sponsorship or standing within the organization to initiate enterprise-wide changes or discussions
- ▶ Peers are often siloed and suspicious of intrusions into "their" sphere of influence



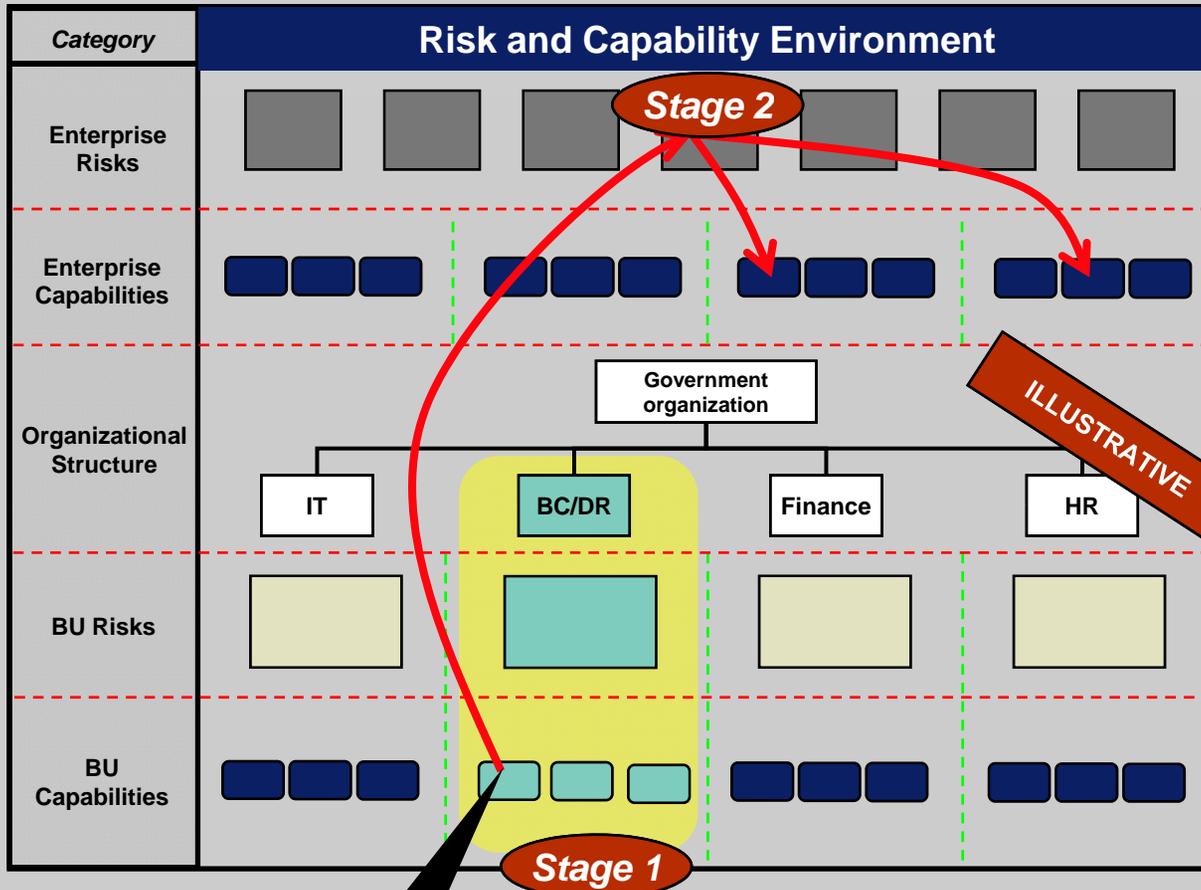
Common Functional Responses

- ▶ Accept limitations on BU's ability to execute its role / mission
 - Blame senior management
 - Blame other BUs
- ▶ Develop capabilities to address inadequacies in the rest of the organization
 - Duplicative investments and activities
 - Breeds resentment and reinforces territorial confrontations

Instead, use SRM to improve BU risk management, better achieve BU mission, and drive organization-wide improvements



...using a 2-stage approach to link a sub-organization's risks and capabilities to the rest of the organization



BU capability dependent on enterprise capabilities managed by other parts of the organization

- ### "2-Stage" SRM Methodology
- ▶ Risks and capabilities are identified, prioritized, and assessed in two stages
 - 1** First, focus on risks to the BU mission and the capabilities it has in place to mitigate them
 - 2** Then, identify obstacles (risks) to the effective implementation of the BU capabilities
 - ▶ Doesn't require participation / agreement of the entire organization
 - ▶ Doesn't require senior management participation / direction
 - ▶ Risk Architecture step can focus on either BU or enterprise level processes and can include other participating BUs
 - ▶ Enterprise risks identified can be used to inform senior leadership agenda in full or selectively

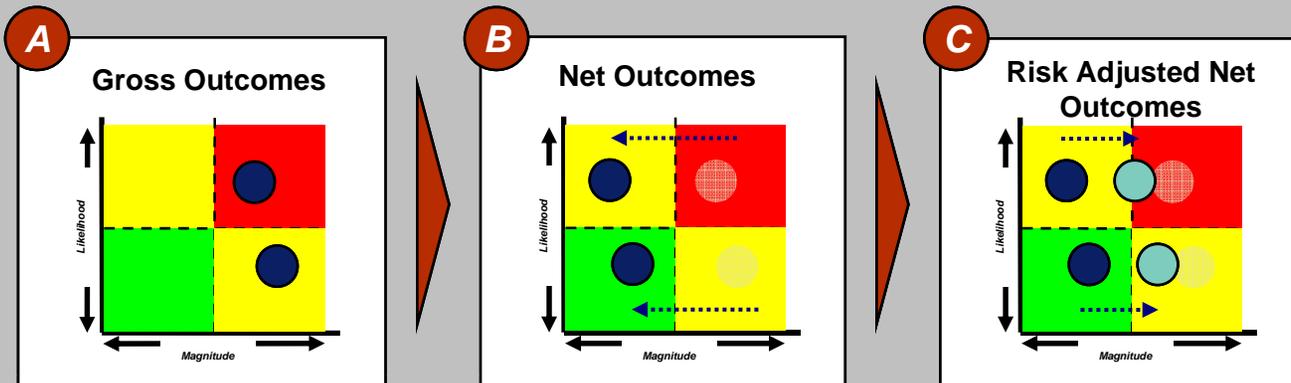


We demonstrated the functional SRM concept on an engagement for a government organization's BC/DR office...

Client Challenge

- ▶ Brought in to mature BC/DR program after major BC/DR issues had already been resolved
- ▶ Remaining major obstacles to BC/DR maturity involved coordination with other BUs, enterprise risks, and the immaturity of other organizational capabilities
- ▶ Clarify how risk management activities improve the organization's ability to deliver services
- ▶ Develop governance process for risk that defines the roles, responsibilities, accountability, and decision rights for senior management

Stage 1 Risk Prioritization

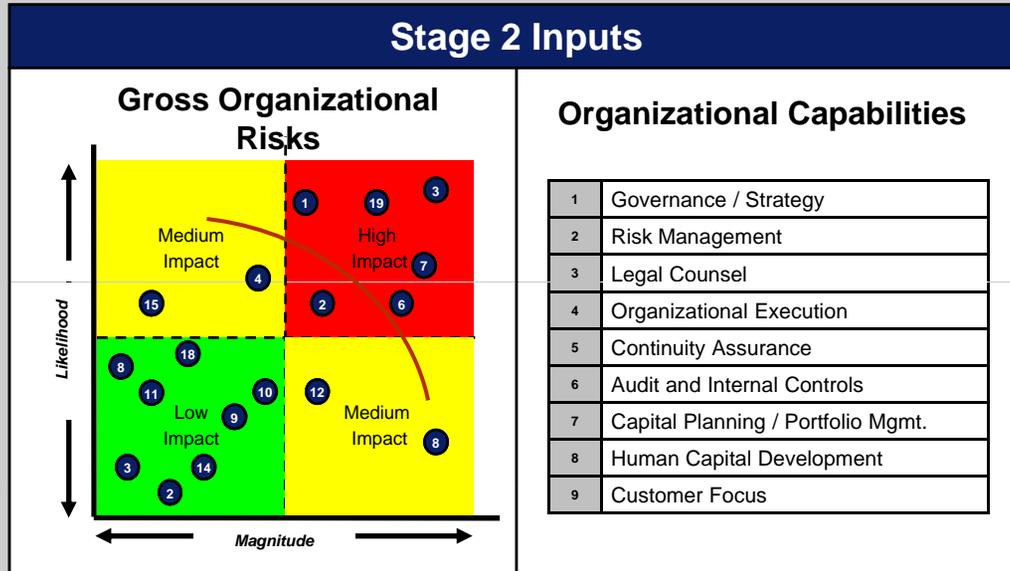


Stage 1 Outputs

- ▶ Prioritize BC/DR activities
- ▶ Justify functional capability investments
- ▶ Address BC/DR-specific challenges



...beginning with BU challenges and ending up helping to set the cross-organization strategic agenda



- ### Stage 2 Results
- ▶ Politically-safe mechanism for BU management client to address organizational inefficiencies in other BUs
 - ▶ Increase client stature in cross-organizational forums (CPIC, strategy development)
 - ▶ Refinement of strategic objectives
 - ▶ Directly identifies which capabilities “buy down” the most BC/DR risk



Contact Information

▶ Ernest W. Wohnig III, PMP

- ◆ Portfolio Manager Energy and Environment Sectors
- ◆ Booz Allen Hamilton
- ◆ Ph: (703) 377-1249
- ◆ E-mail: wohnig_ernest@bah.com



QUESTIONS



Supplemental Slides



Risk identification begins with interviews and external research to better understand client organization and context...

Methodology

Approach

Interviews	<ul style="list-style-type: none">▶ Establish consistent lexicon and syntax▶ Coordinate if using parallel interview teams (e.g., interview guide, interim reviews)▶ Document interview notes and sources▶ Group risks based on level and/or category
History / Document	<ul style="list-style-type: none">▶ Leverage outputs of existing or previous analyses▶ Analyze existing data to forecast potential obstacles
Structured External Insight	<ul style="list-style-type: none">▶ Identify and gather input from industry and government experts outside of our core team▶ Explore potential for partnering or teaming with subject matter experts (SME) outside of Booz Allen



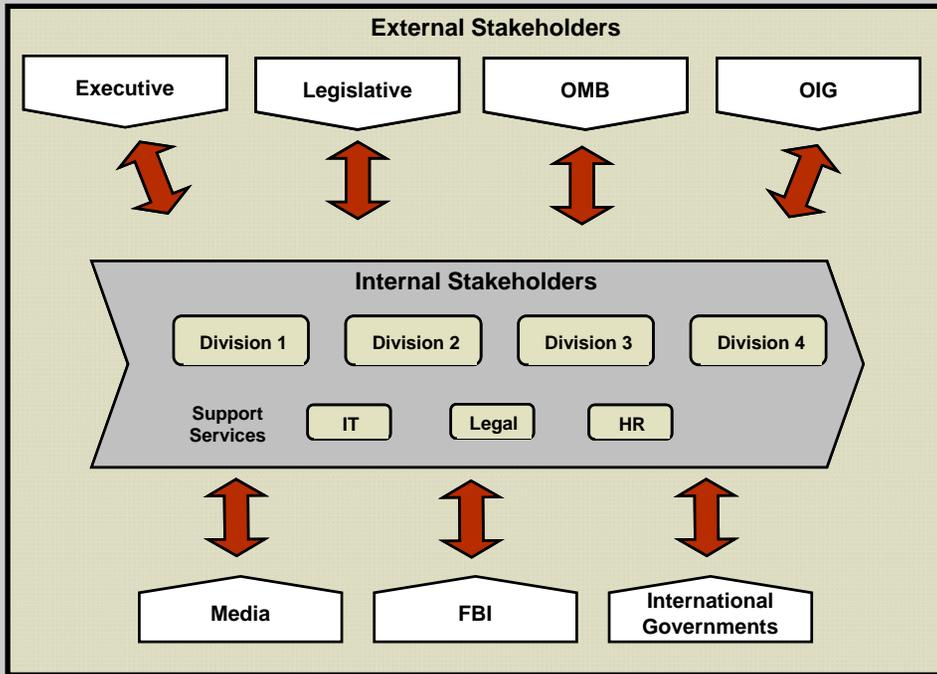
Initial Risk List
<ul style="list-style-type: none">▶ Compile from multiple sources▶ Coordinate brainstorming sessions to hypothesize and mitigate risks which are proved incorrect or unsubstantiated▶ Begin to standardize risk levels by dividing or combining similar risks▶ Recognize themes or repeated priorities▶ Group and categorize risks using various criteria to check for coverage gaps▶ Seek validation on initial lists from key clients and stakeholders



...supplemented with structured identification frameworks to discover hidden risks and ensure comprehensiveness



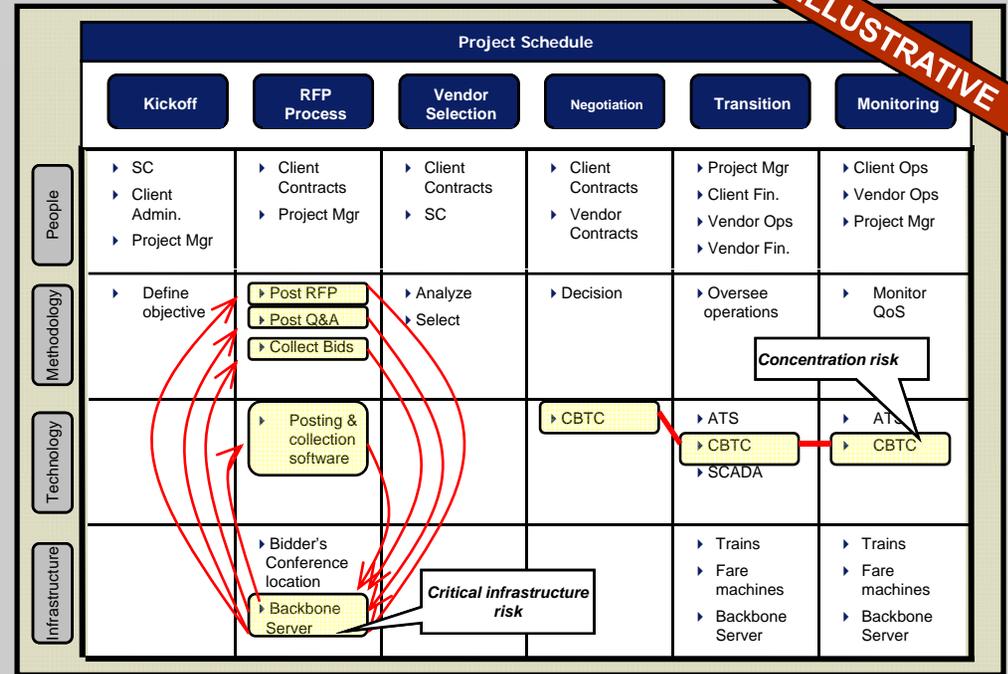
Stakeholder Framework



Benefits

- ▶ Developed specifically for the organization being analyzed
- ▶ Analyzes the interactions between pair wise combinations of all internal and external stakeholders
- ▶ Ensures all stakeholder concerns are addressed

Task ID / Process Flow



Benefits

- ▶ Maps critical assets to each phase of a project
- ▶ Uncovers critical infrastructure and concentration risks

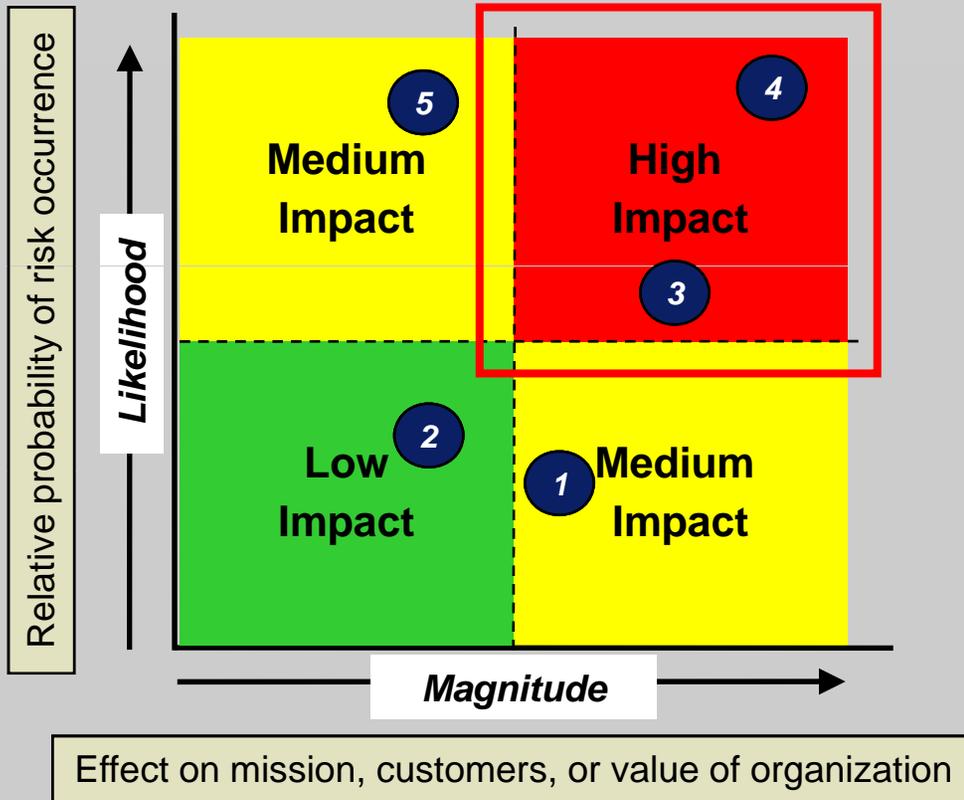
Ernest W. Wohnig III

August 9-12, 2009



Structured prioritization of the identified risks generates consensus around the largest risks to the organization

Gross Risk "Heat Map"



Risk Prioritization Benefits

- ▶ Provides transparency into management priorities / decision-making
- ▶ Justifies resource allocation decisions
- ▶ Generates consensus about largest risks across organization (avoids disparate priorities)
- ▶ Determines granularity and rigor of quantification by type of risks and the specifics of the client situation
- ▶ Can be done at BU or enterprise level or both sequentially

Risk List

1	Targeted Messaging attacks (e.g. Phishing, P2P, Instant Messaging) on internal systems allow secretive command-and-control by a botnet
2	Close proximity transmission intercepts (e.g. via Blackberry, laptop, wireless access point) permit intrusion into core LAN infrastructure
3	Increasingly sophisticated malicious code embedded in Web 2.0 websites allows system exploitation opportunities
4	Mission essential IT systems that use COTS-based software introduce publicly available security vulnerabilities
5	Compromised hardware / software introduced into local environment due to adversaries involved in the supply chain process

Notional

Identified Risks



For clients without market capitalizations (i.e. government), magnitude quantification often utilizes essential functions / outputs

A Identify Essential Functions / Outputs

- ▶ Distinguish key activities that are vital to the organization's operations and/or mission
- ▶ Gather input from key stakeholders, management, and risk identification activities

EXAMPLE

Essential Function / Outputs	Risk 1	Risk 2	Risk 3
Provide legal counsel and guidance			
Provide response capabilities			
Order goods and services			
Assure funds availability			
Pay people and vendors			
Assure system availability			
Process payroll and employee benefits			
Average	X	Y	Z

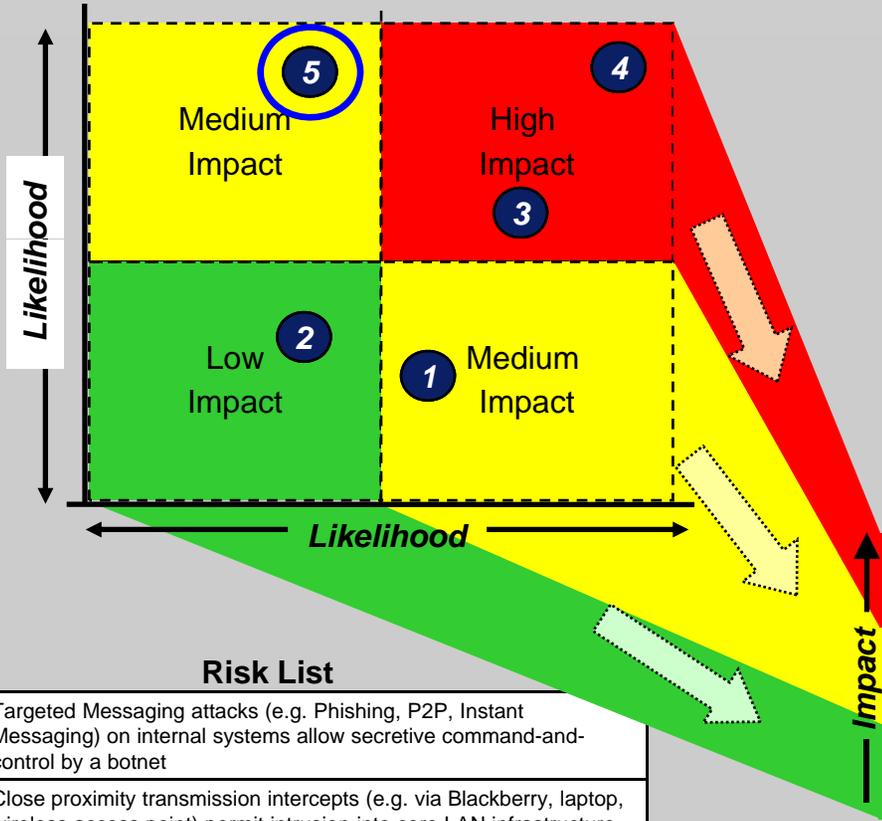
B Assess Effects for Each Risk

- ▶ Assign scores to each essential function to determine how each risk adversely affects the organizations' ability to perform that essential function
- ▶ Use a weighted or simple average of essential functions to calculate the magnitude for each risk
- ▶ Clearly document assumptions/sources for each assessment



Fully characterizing a client's existing capabilities emphasizes forward thinking responses and provides insight into how to most efficiently reduce risk

A Group the Prioritized Risks

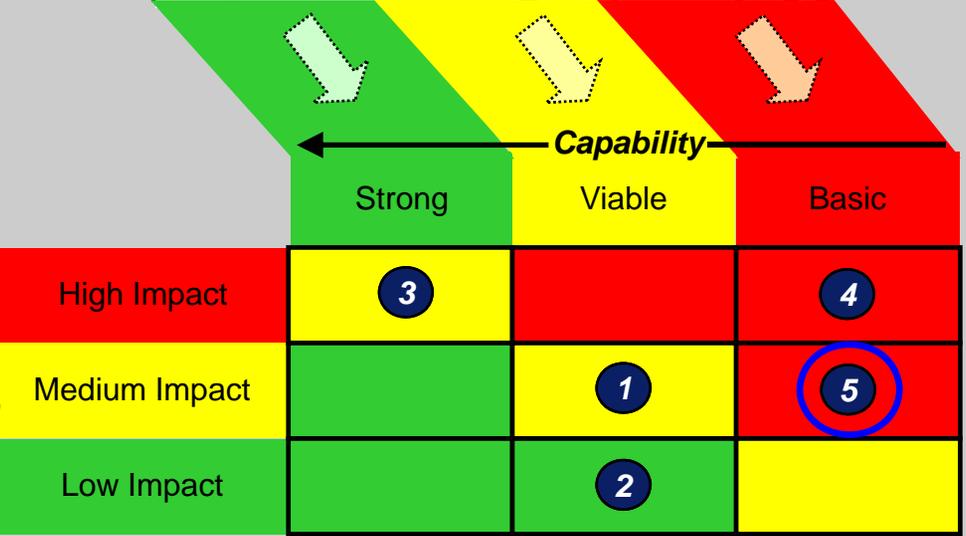


Risk List	
1	Targeted Messaging attacks (e.g. Phishing, P2P, Instant Messaging) on internal systems allow secretive command-and-control by a botnet
2	Close proximity transmission intercepts (e.g. via Blackberry, laptop, wireless access point) permit intrusion into core LAN infrastructure
3	Increasingly sophisticated malicious code embedded in Web 2.0 websites allows system exploitation opportunities
4	Mission essential IT systems that use COTS-based software introduce publicly available security vulnerabilities
5	Compromised hardware / software introduced into local environment due to adversaries involved in the supply chain process

B Assess Mitigating Capabilities

Strong	Viable	Basic
<ul style="list-style-type: none"> Security Infrastructure Business Continuity Federated Access 	<ul style="list-style-type: none"> Procurement Efficiency Location Independent IT Agile Networks 	<ul style="list-style-type: none"> Workstation Strategy Technology Insertion IT Customer Support

Capabilities that mitigate Risk #5



C Map Capabilities to Risks



This is done by appropriate stakeholders assessing the relative strengths and weaknesses of the organization

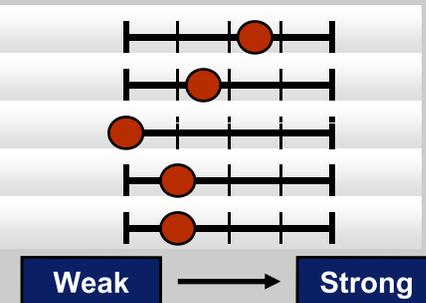
Capabilities

1	Governance / Strategy
2	Risk Management
3	Legal Counsel
4	Organizational Execution
5	Information Technology
6	Audit and Internal Controls
7	Capital Planning / Portfolio Mgmt.
8	Human Capital Development
9	Customer Focus
10	Assets and Logistics
11	Continuity Assurance

IT Sub-Capabilities

- Federated Access
- Soft Copy
- Holdings Management
- Ubiquitous Access
- Single Customer View

Relative Sub-Capability Assessments



Capabilities are the inherent capabilities needed for a client to accomplish its mission

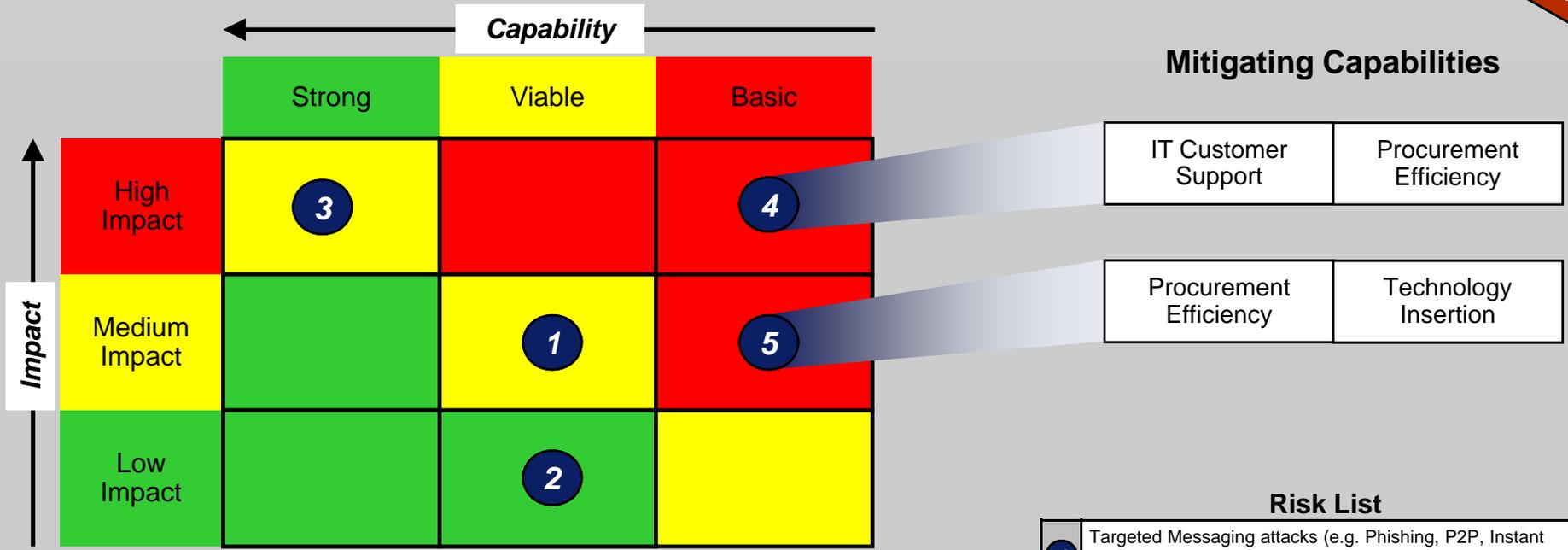
Each Capability is comprised of sub-capabilities that should be assessed separately (often grouped by people, process, technology)

Assessments are generally internally referential and are intended to help prioritize between risks



Combining the results of grouped impacts and capabilities generates the organization's comprehensive "net" risk agenda

ILLUSTRATIVE



Mitigating Capabilities

IT Customer Support	Procurement Efficiency
Procurement Efficiency	Technology Insertion

Risk List

1	Targeted Messaging attacks (e.g. Phishing, P2P, Instant Messaging) on internal systems allow secretive command-and-control by a botnet
2	Close proximity transmission intercepts (e.g. via Blackberry, laptop, wireless access point) permit intrusion into core LAN infrastructure
3	Increasingly sophisticated malicious code embedded in Web 2.0 websites allows system exploitation opportunities
4	Mission essential IT systems that use COTS-based software introduce publicly available security vulnerabilities
5	Compromised hardware / software introduced into local environment due to adversaries involved in the supply chain process



The risk architecture step embeds the risk agenda process into existing organizational structures and processes...

Organization

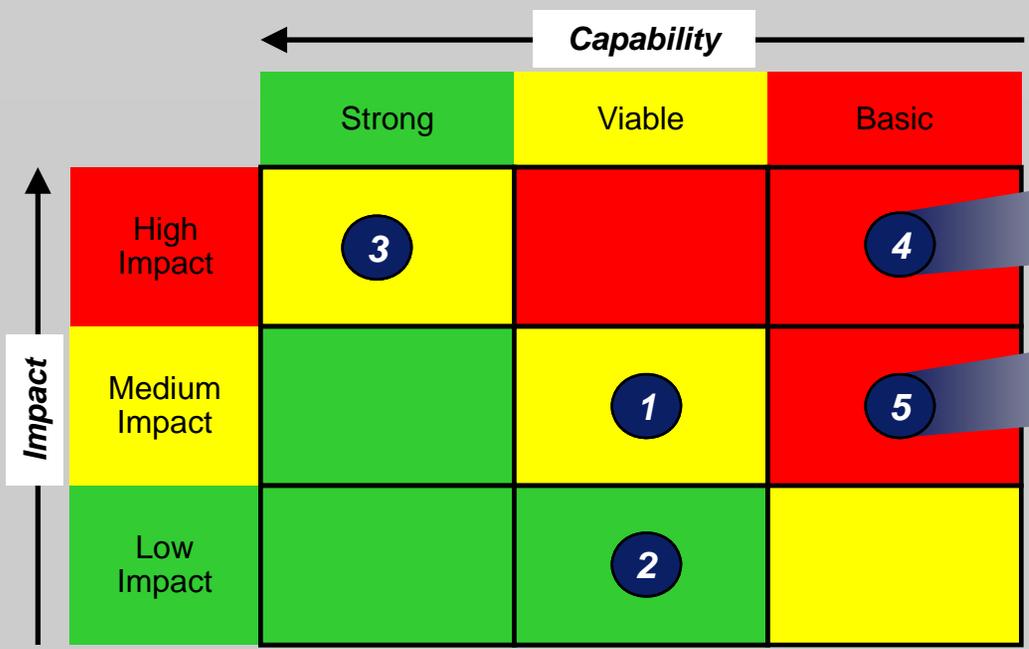
- ▶ Identify optimal structure for client's Risk Management function (e.g., embedded vs. centralized) within existing organizational structures
- ▶ Ensure proper governance / oversight of risk management structures
- ▶ Identify roles and responsibilities for key Risk Management positions
- ▶ Ensure client organizational culture fosters risk management objectives (e.g., risk appetite, collaboration)

Process

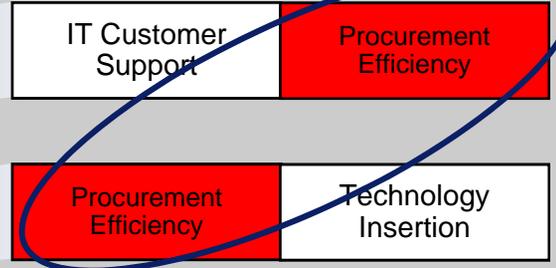
- ▶ Identify opportunities to embed required risk management processes into existing management processes:
 - Risk identification
 - Aggregation
 - Quantification & prioritization
 - Capability assessment
 - Risk agenda development
- ▶ Where new processes are required, identify key roles, steps, linkages, accountabilities, and timing
- ▶ Coordinate with strategic and operating planning processes as necessary – i.e., ensure proposed capability initiatives can be included in upcoming operating plans



The risk agenda is then leveraged to prioritize potential mitigation activities, helping set the organization's strategic agenda



Mitigating Capabilities



ILLUSTRATIVE

Risk List

1	Targeted Messaging attacks (e.g. Phishing, P2P, Instant Messaging) on internal systems allow secretive command-and-control by a botnet
2	Close proximity transmission intercepts (e.g. via Blackberry, laptop, wireless access point) permit intrusion into core LAN infrastructure
3	Increasingly sophisticated malicious code embedded in Web 2.0 websites allows system exploitation opportunities
4	Mission essential IT systems that use COTS-based software introduce publicly available security vulnerabilities
5	Compromised hardware / software introduced into local environment due to adversaries involved in the supply chain process

Prioritized List of Capabilities that Would Buy-Down the Most Risk

1	Procurement Efficiency
2	IT Customer Support
3	Technology Insertion
4	Workstation Strategy