

Risk-to-Mission Assessment Process (RiskMAP)

Presented by Clifford Glantz, PNNL
on behalf of

Jim Watters, MITRE
jwatters@mitre.org
781-271-2162

Peter Kertzner, MITRE
kertzner@mitre.org
781-271-2286

This work was supported under Award number 2003-TK-TX-0003 from the U.S. Department of Homeland Security, Science and Technology Directorate. Points of view in this document are those of the authors and do not necessarily represent the official position of the U.S. Department of Homeland Security or the Science and Technology Directorate. The I3P is managed by Dartmouth College.

Approved for Public Release; Distribution Unlimited. MITRE No. 06-0760. Copyright © 2006 by the Trustees of Dartmouth College. The I3P Logo is a trademark of Dartmouth College. All information contained in this document may not be reproduced without permission by the I3P.

Questions

◆ You're doing an API-NPRA Security Vulnerability Assessment

- How do you pick your most critical assets?
...or your most critical functions?
...or your most critical interdependencies?

◆ Your Red Team says you have vulnerabilities

- Which ones do you fix?
- How much is enough?
- Where are the risks?

Where Are Your Corporate Risks?

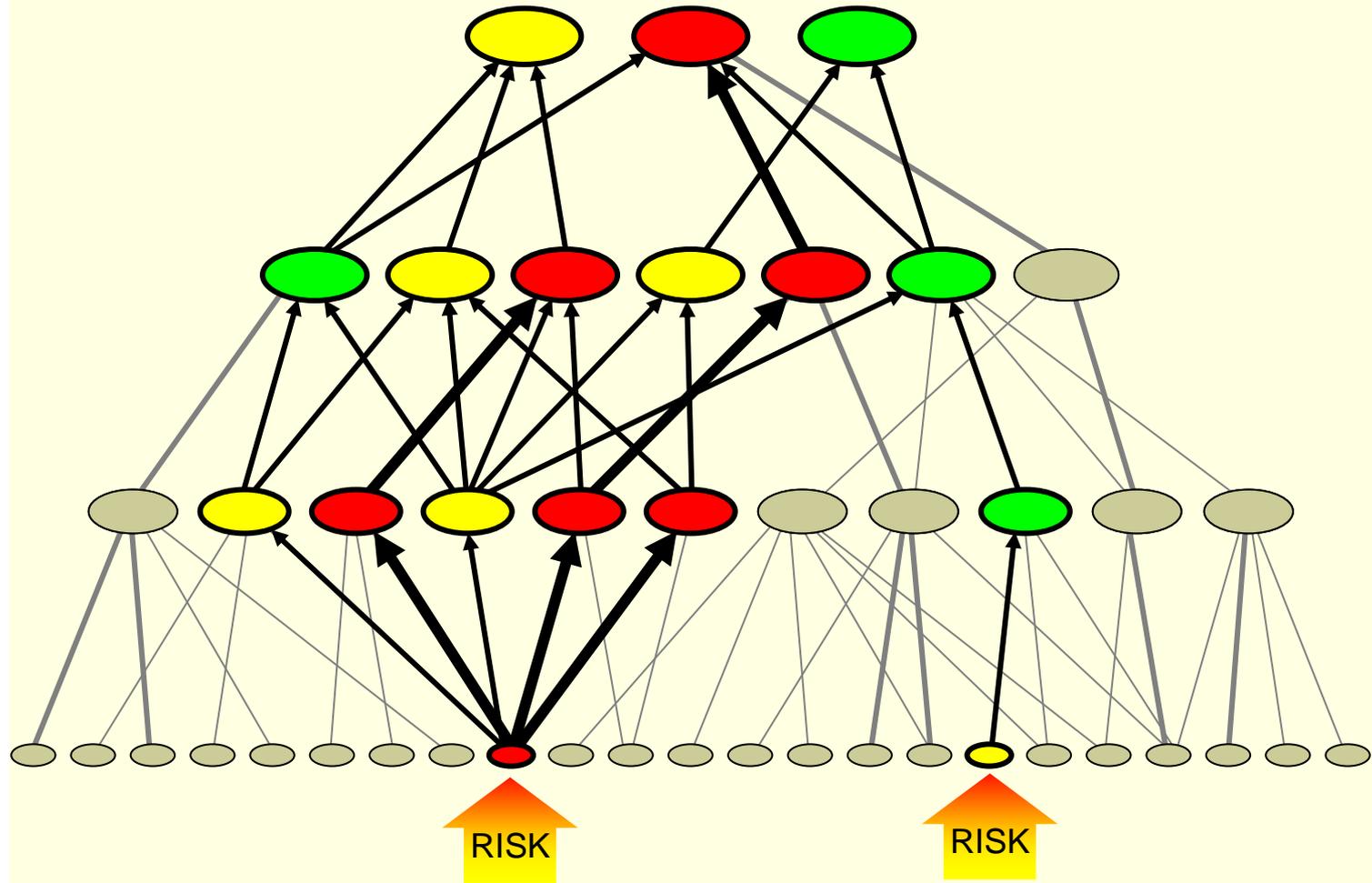
How to figure all of this out??? Use RiskMAP!

Business Objectives

Operational Tasks

Information Assets

Network Nodes



What is RiskMAP?

◆ Risk-to-Mission Assessment Process

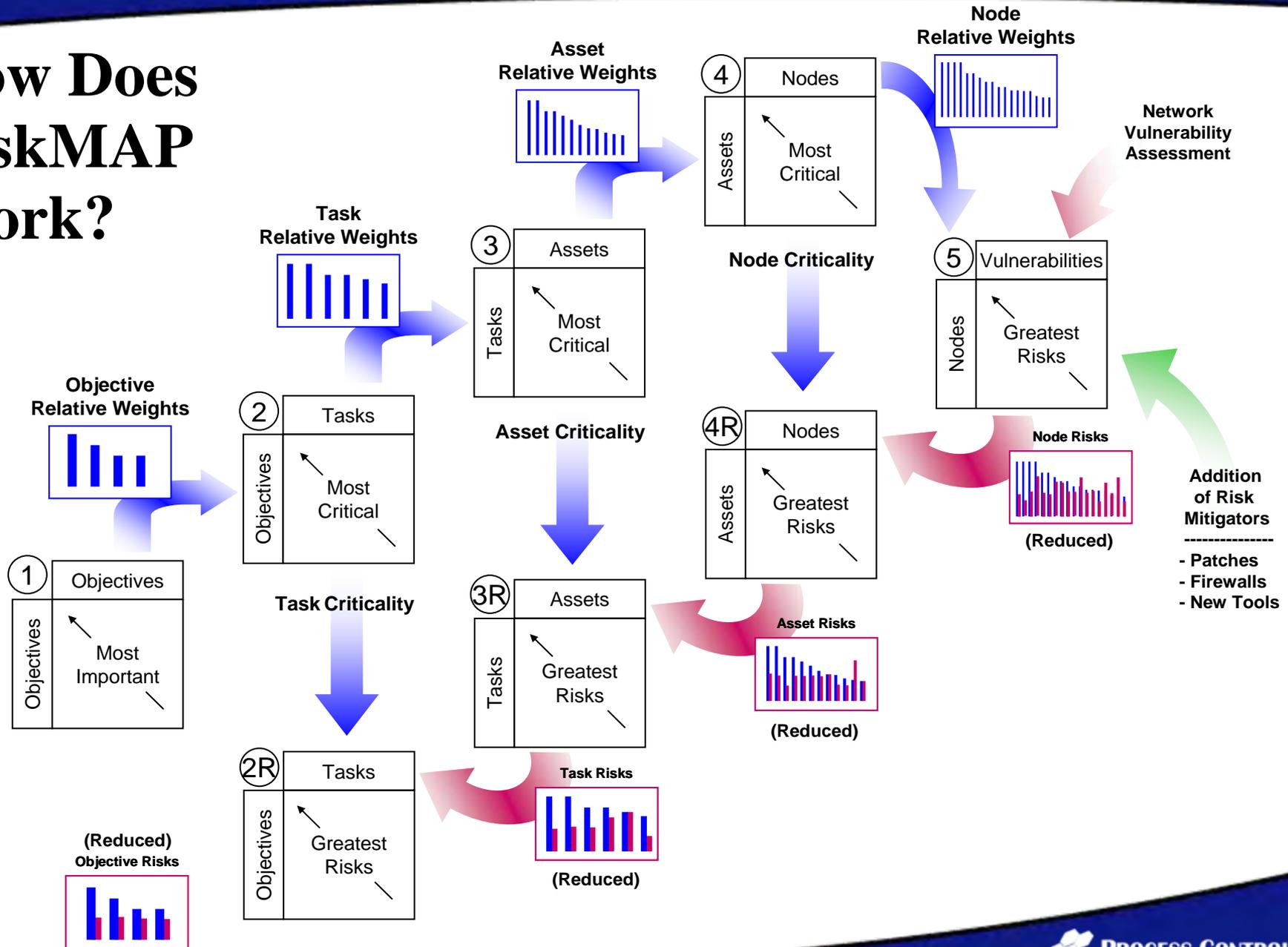
◆ What it does:

- Models a business's pertinent features
- Maps between network risk and business risk
- Provides solid decision support for the CIO

◆ What it doesn't do:

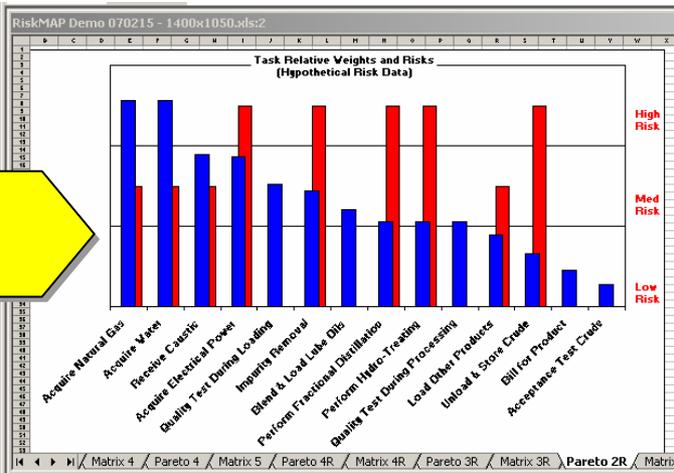
- Scan for vulnerabilities
- Generate network risk values

How Does RiskMAP Work?

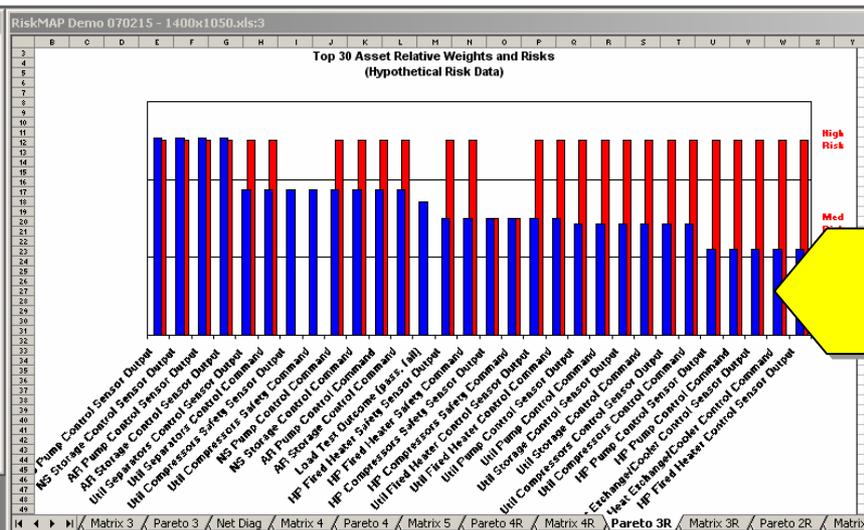


Dashboard View – Before Mitigation

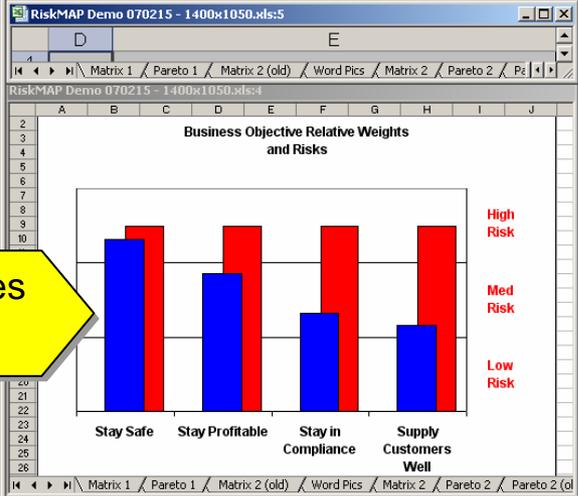
Tasks
 ■ Weights
 ■ Risks



Assets
 ■ Weights
 ■ Risks



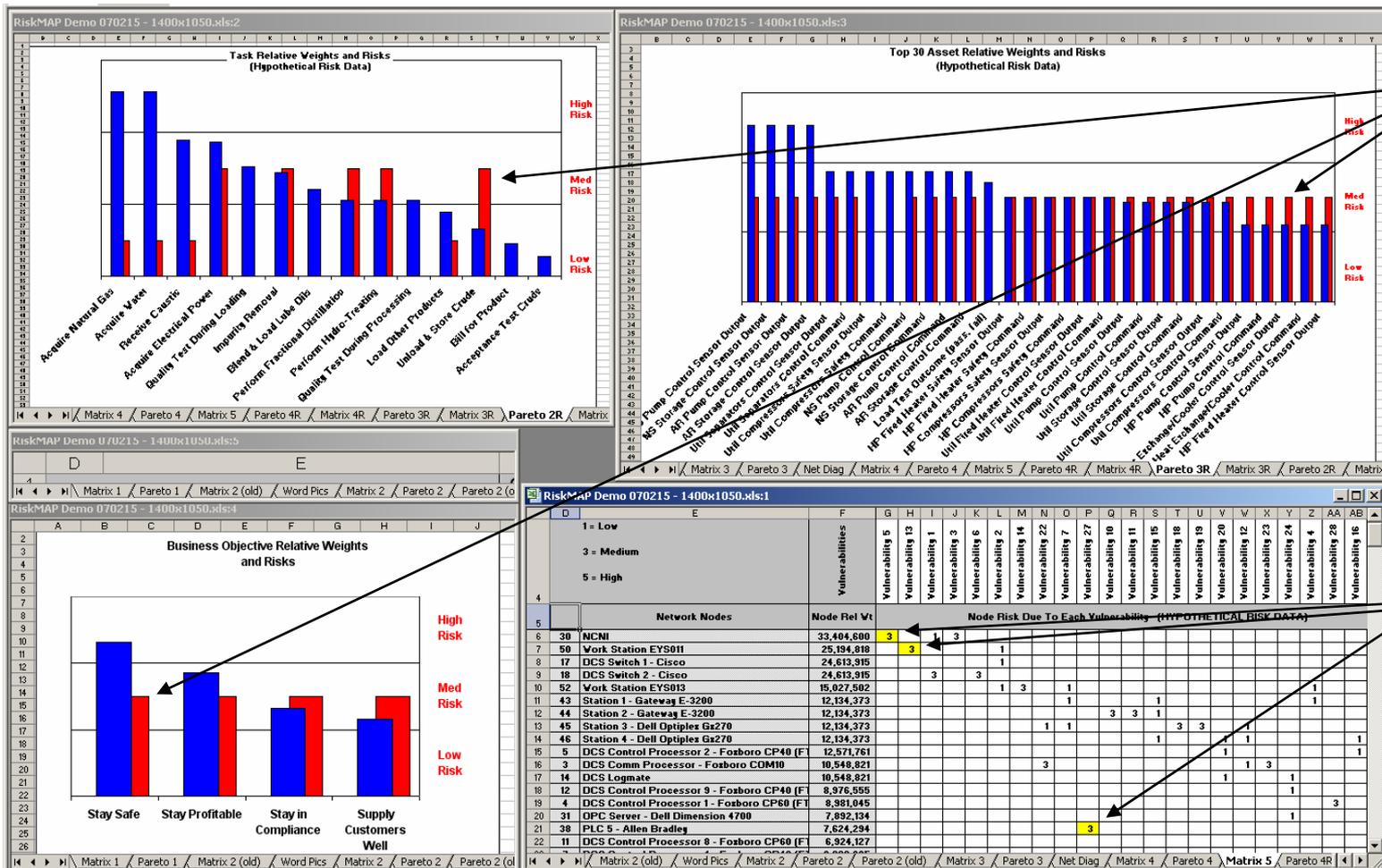
Objectives
 ■ Weights
 ■ Risks



Network Node Risks

1 = Low 3 = Medium 5 = High		Vulnerabilities		G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	AA	AB	AC	
				Vulnerability 5	Vulnerability 13	Vulnerability 1	Vulnerability 3	Vulnerability 6	Vulnerability 2	Vulnerability 14	Vulnerability 22	Vulnerability 7	Vulnerability 27	Vulnerability 10	Vulnerability 11	Vulnerability 15	Vulnerability 16	Vulnerability 19	Vulnerability 20	Vulnerability 23	Vulnerability 24	Vulnerability 4	Vulnerability 28	Vulnerability 16	Vulnerability 9		
				Network Nodes																							
				Node Rel Vt																							
				Node Risk Due To Each Vulnerability (HYPOTHETICAL RISK DATA)																							
6	30	NCNI	33,404,600	5		1	3																				
7	50	Work Station EYS011	25,194,818		5				1																		
8	17	DCS Switch 1 - Cisco	24,613,915							1																	
9	18	DCS Switch 2 - Cisco	24,613,915			3	3																				
10	52	Work Station EYS013	15,027,502						1	3		1														1	
11	43	Station 1 - Gateway E-3200	12,134,373											3	3	1											
12	44	Station 2 - Gateway E-3200	12,134,373																								
13	45	Station 3 - Dell Optiplex Gz270	12,134,373														1	3	3								
14	46	Station 4 - Dell Optiplex Gz270	12,134,373														1							1	1		
15	5	DCS Control Processor 2 - Foxboro CP40 (F)	12,571,761																							1	
16	3	DCS Comm Processor - Foxboro COM10	10,548,821									3													1	3	
17	14	DCS Logmate	10,548,821																							1	
18	12	DCS Control Processor 9 - Foxboro CP40 (F)	8,976,555																							1	
19	4	DCS Control Processor 1 - Foxboro CP60 (F)	8,981,045																							1	
20	31	OPC Server - Dell Dimension 4700	7,892,134																							1	
21	38	PLC 5 - Allen Bradley	7,624,294																							1	
22	11	DCS Control Processor 8 - Foxboro CP60 (F)	6,924,127										5													1	

Dashboard View – After Mitigation



Reduced Risks Based on Modeled Relationships

Addition of Risk Mitigators

Are the Results Credible? Useful?

◆ Credibility of Results

- Model based wholly on Owner/Operator input
- Network risks input by company's own experts
- Drill-down to risk sources is quick & traceable

◆ Utility of Results

- Model is reusable for future assessments
- Results support various operations decisions
- Refinery template used by Ergon Refining, Inc.

What's Next for RiskMAP?

- ◆ **Topics for further development include:**
 - Additional data template(s)
 - Inclusion of Confidentiality issues in analysis

- ◆ **Commercialization of prototype is underway**
 - Seeking qualified developers through Fluid Innovation Group
 - Contact Andrew Allemann at (512) 437-2427 or allemann@fluidinnovation.com

Summary

- ◆ RiskMAP enables accurate identification of critical functions, assets, and network nodes.
- ◆ RiskMAP provides CIO-level decision support including drill-down and what-if exercises.
- ◆ Detailed info available at the I3P web site www.thei3p.org