The Ninth National HIPAA Summit™
The Leading Forum on Healthcare Privacy, Confidentiality, Data Security and HIPAA Compliance

Security Standards Workshop: An Overview – From Risk Assessment to Proposed Policies

Presenter:

Frank Ruelas, MBA

Director, Corporate Compliance
Gila River Health Care Corporation
Sacaton, Arizona

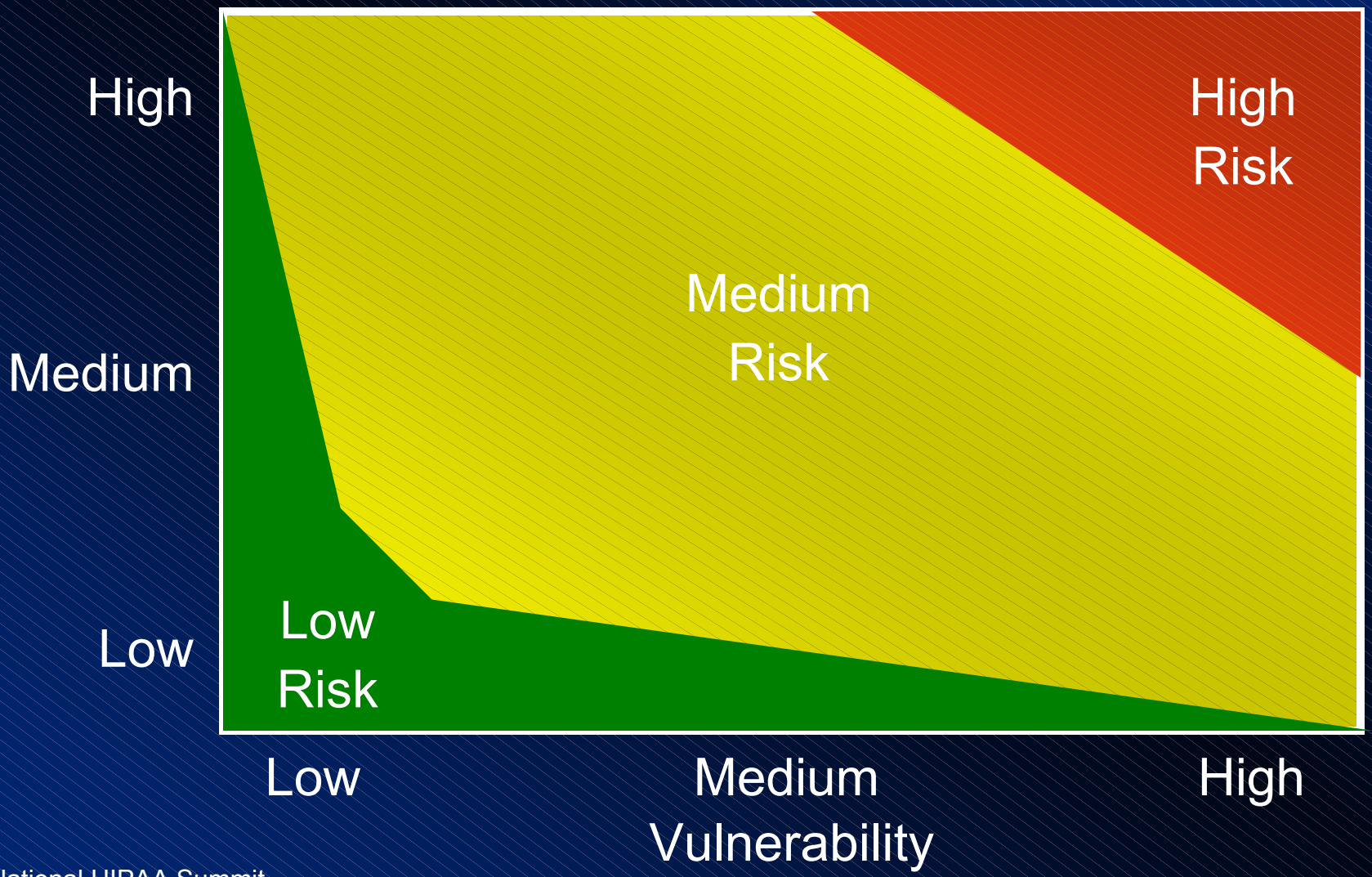
September 12, 2004

Why are terms so important?

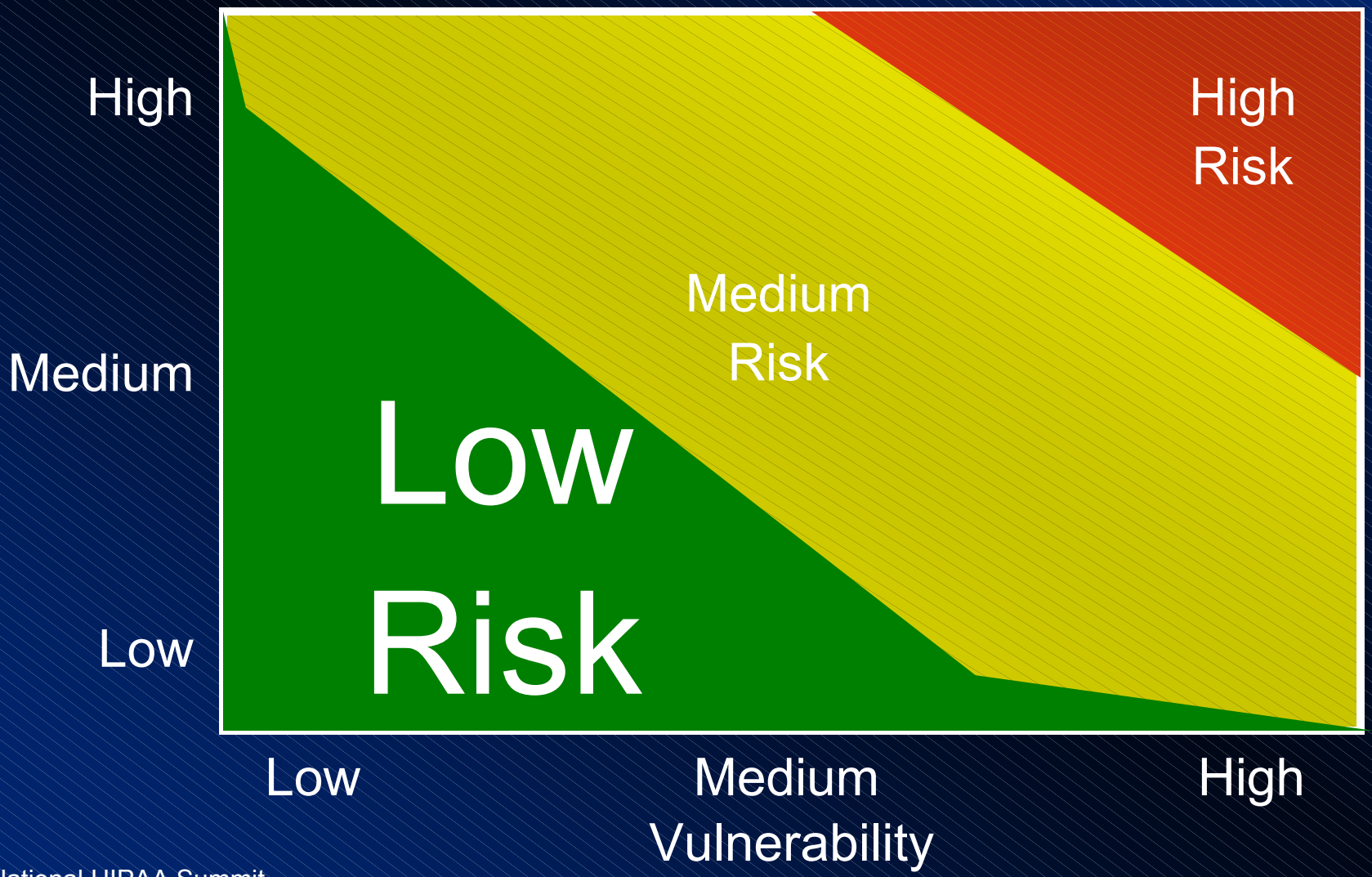
Allows for people to develop and operate from a common point of reference.

- Threat
  - An action or situation that may exploit a vulnerability
- Vulnerability
  - A flaw or weakness
- Safeguard
  - A control or countermeasure to a vulnerability

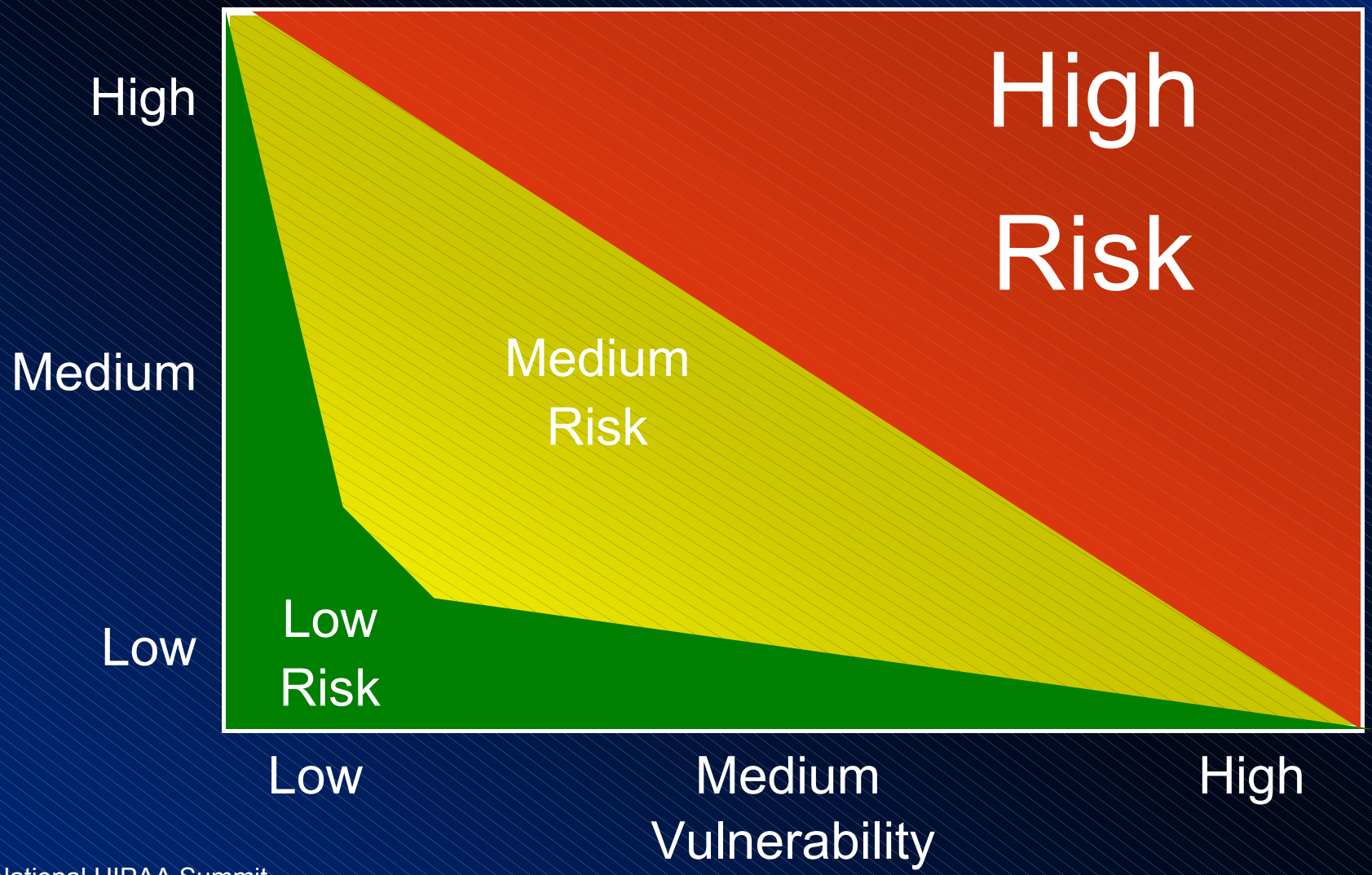
Vulnerability and Threat Relationship



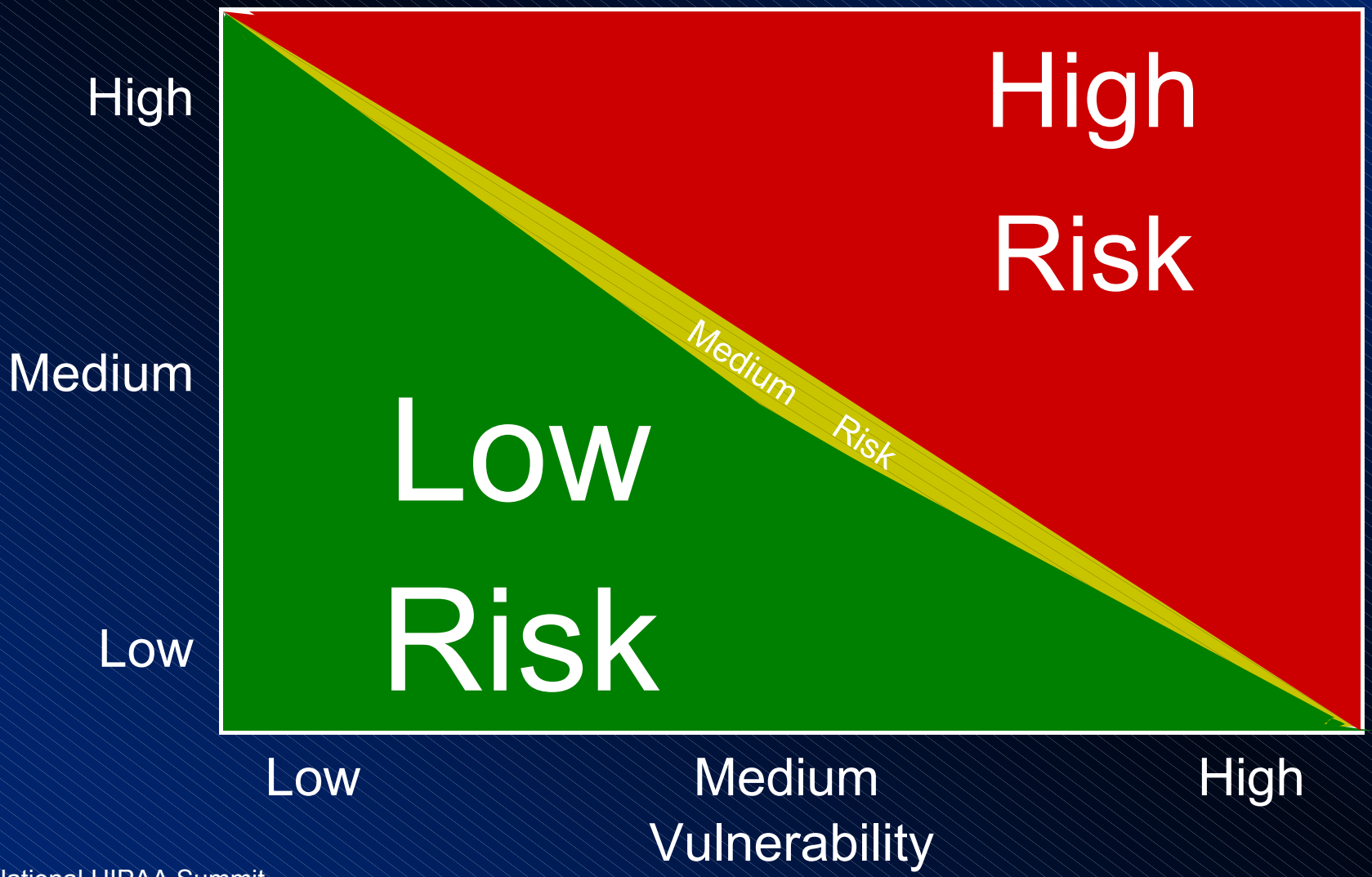
Vulnerability and Threat Relationship



Vulnerability and Threat Relationship



Vulnerability and Threat Relationship



Information Gathering

- Questionnaires
- Interviews
- Organization history
- Document review
- Partnering efforts

Information Gathering

- Questionnaires
- Interviews
- Organization history
- Document review
- Partnering efforts

Information Gathering

- Questionnaires
- Interviews
- Organization history
- Document review
- Partnering efforts

Information Gathering

- Questionnaires
- Interviews
- Organization history
- Document review
- Partnering efforts

Information Gathering

- Questionnaires
- Interviews
- Organization history
- Document review
- Partnering efforts

Outward to Inward Focus Approach

"Staff employees pose perhaps the greatest risk in terms of access and potential damage to critical information systems…Considered 'members of the family,' they are often above suspicion—the last to be considered when systems malfunction or fail."

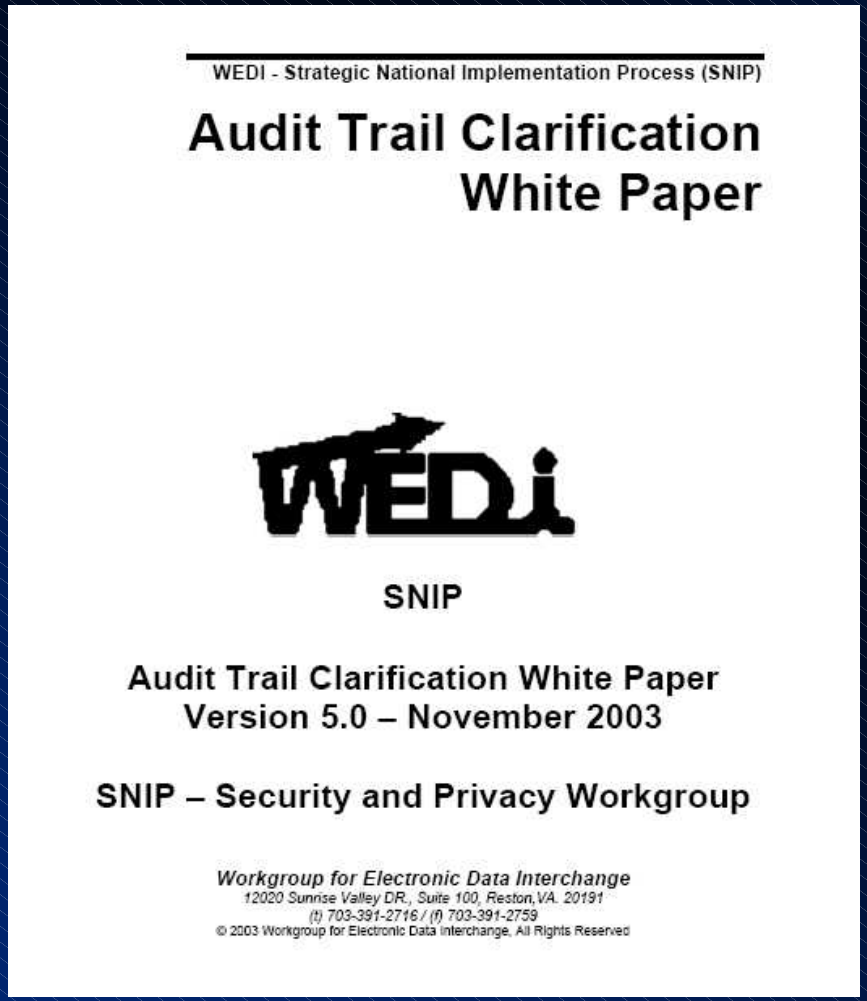
Source: *Security Awareness Bulletin* No. 2-98, Department of Defense Security Institute, September 1998.

Helpful Hint:
Don't overlook part-time or temp staff.

Layers of Security – User Authentication

- The layers refer to:
  - First
    - Something you know
  - Second
    - Something you have
  - Third
    - Something you are

Audit Trail Considerations


WEDI - Strategic National Implementation Process (SNIP)

Audit Trail Clarification White Paper

WEDI

SNIP

Audit Trail Clarification White Paper
Version 5.0 – November 2003

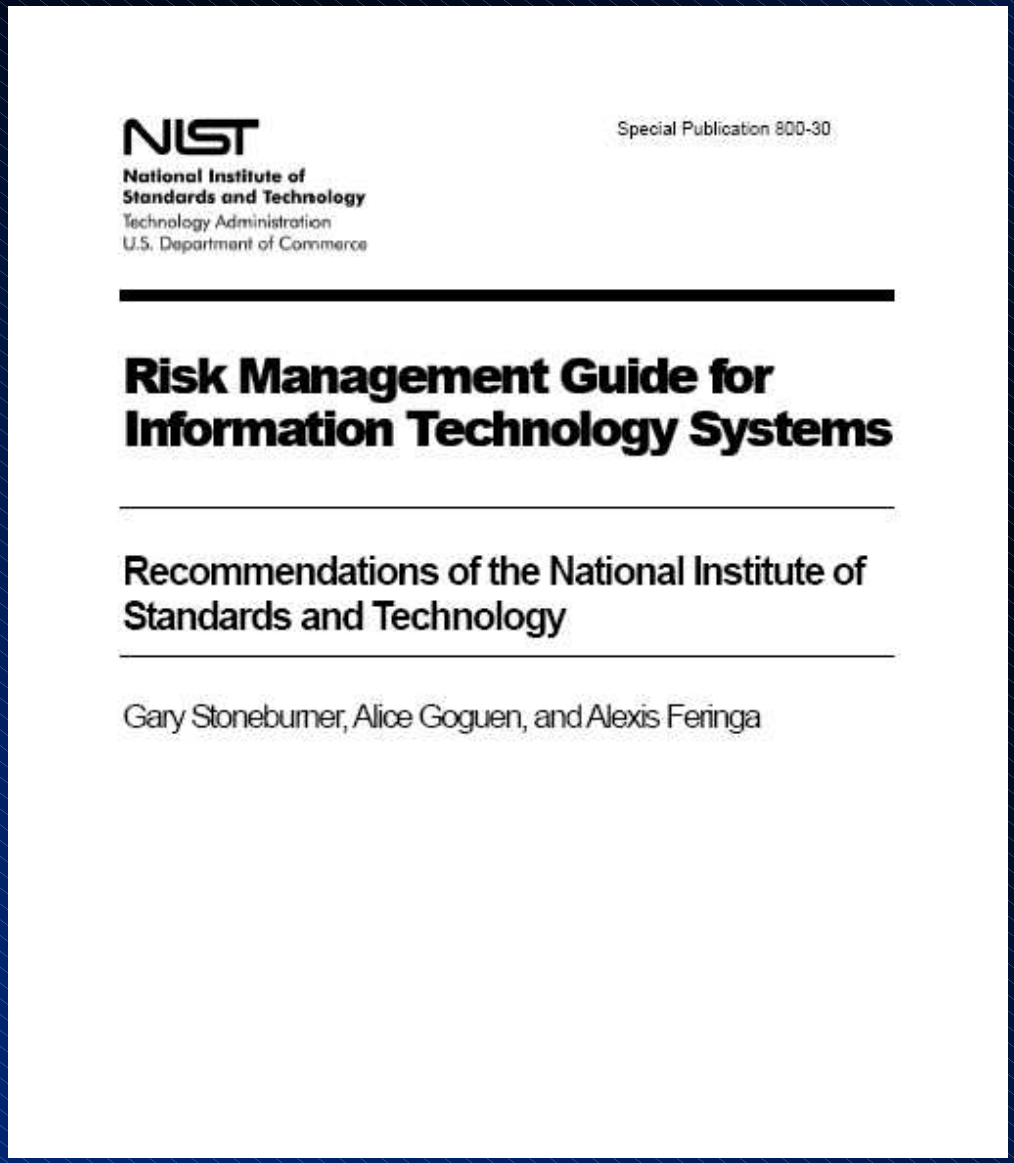
SNIP – Security and Privacy Workgroup

Workgroup for Electronic Data Interchange
12020 Sunrise Valley DR., Suite 100, Reston, VA. 20191
(t) 703-391-2716 / (f) 703-391-2759

"Generally an audit trail identifies Who…did What…to What data…and When."

- Audit controls can be manual, automatic, or a combination of both
- Costs associated include the audit control, implementation, personnel, and hardware.

Rating Methods for Risk Assessment



NIST
National Institute of Standards and Technology
Technology Administration
U.S. Department of Commerce

Special Publication 800-30

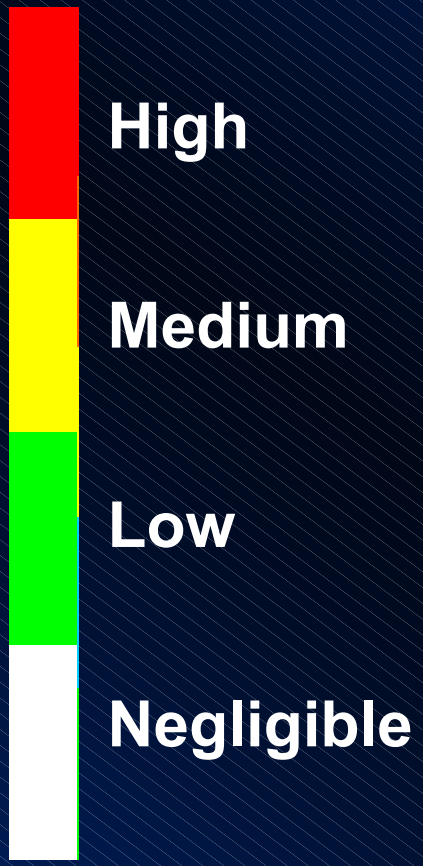
Risk Management Guide for Information Technology Systems

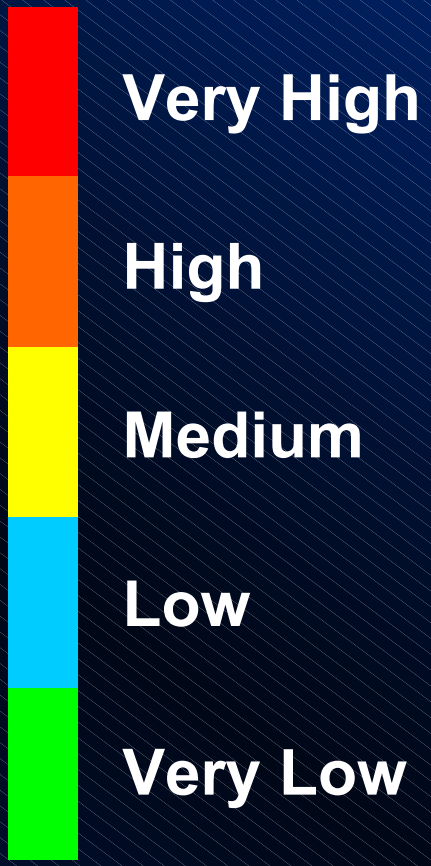
Recommendations of the National Institute of Standards and Technology

Gary Stoneburner, Alice Goguen, and Alexis Feringa

- Quantitative vs. Qualitative discussion
- Provides a perspective on rating levels
  - High
  - Medium
  - Low
- Uses a matrix approach to categorize risk levels

Level Description - Examples





Risk Assessment Calculations

- Create a matrix framework that will be used to determine risk levels with the probability of a threat occurring as one axis and the subsequent impact of the threat
  - 3 X 3
  - 4 X 4
  - 5 X 5
- Assign numerical values to the levels used to create the matrix
  - Threat values: 1 / (number of levels)
  - Impact values: 100 / (number of levels)

High 1.00			
Medium .50			
Low .10			
	Low 10	Medium 50	High 100

Very High 1.00					
High .80					
Medium .60					
Low .40					
Very Low .20					
	Very Low 20	Low 40	Medium 60	High 80	Very High 100

Risk Matrices Examples

High 1.00			
Medium .50			
Low .10			
	Low 10	Medium 50	High 100

3 X 3

- Low 1 to 10
- Medium >10 to 50
- High >50 to 100

High 1.00				
Medium .80				
Low .60				
Negligible .40				
	Negligible 20	Low 40	Medium 60	High 80

4 X 4

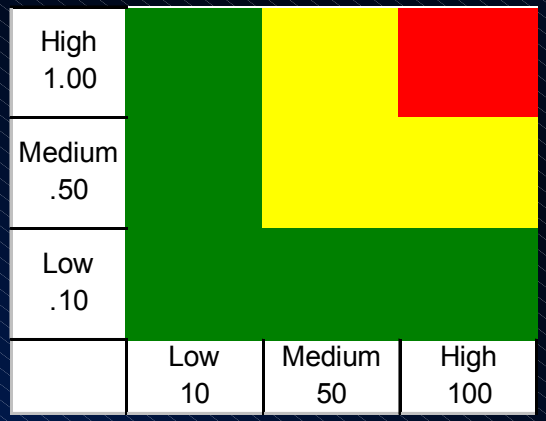
- Negligible 1 to 25
- Low >25 to 50
- Med >50 to 75
- High >75 to 100

5 X 5

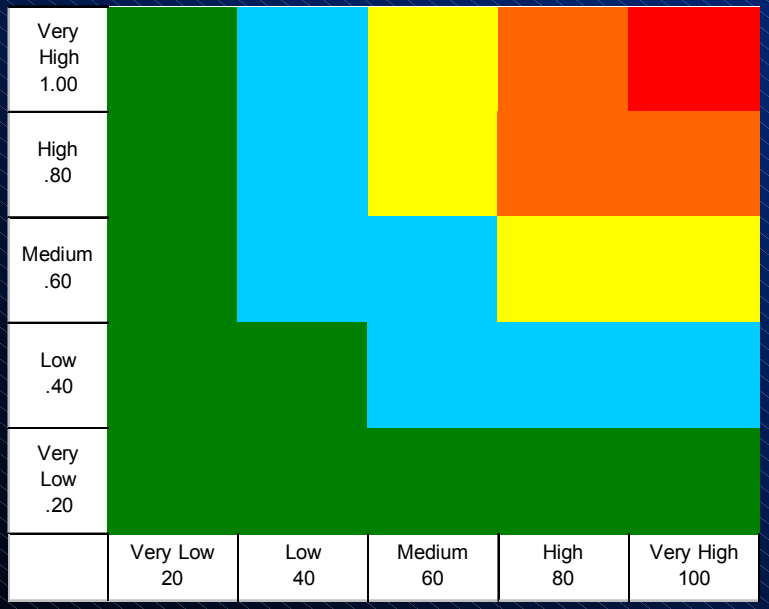
- Very Low 1 to 20
- Low >20 to 40
- Med >40 to 60
- High >60 to 80
- Very High >75 to 100

Very High 1.00					
High .80					
Medium .60					
Low .40					
Very Low .20					
	Very Low 20	Low 40	Medium 60	High 80	Very High 100

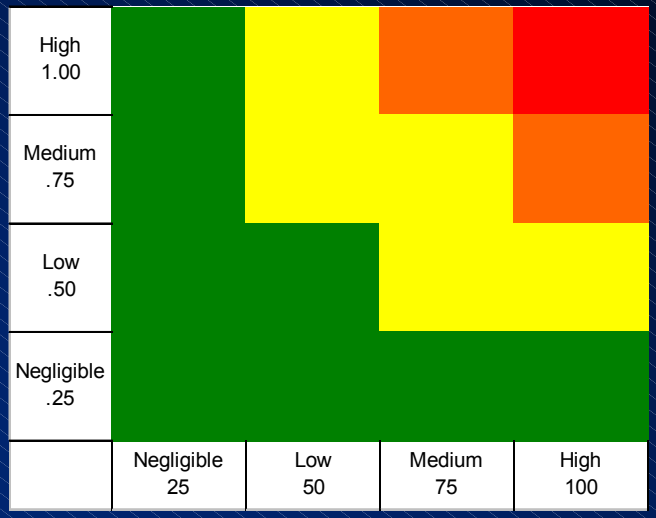
Risk Matrices Examples



3 X 3
Low 1 to 10 (55%)
Medium >10 to 50 (33%)
High >50 to 100 (11%)

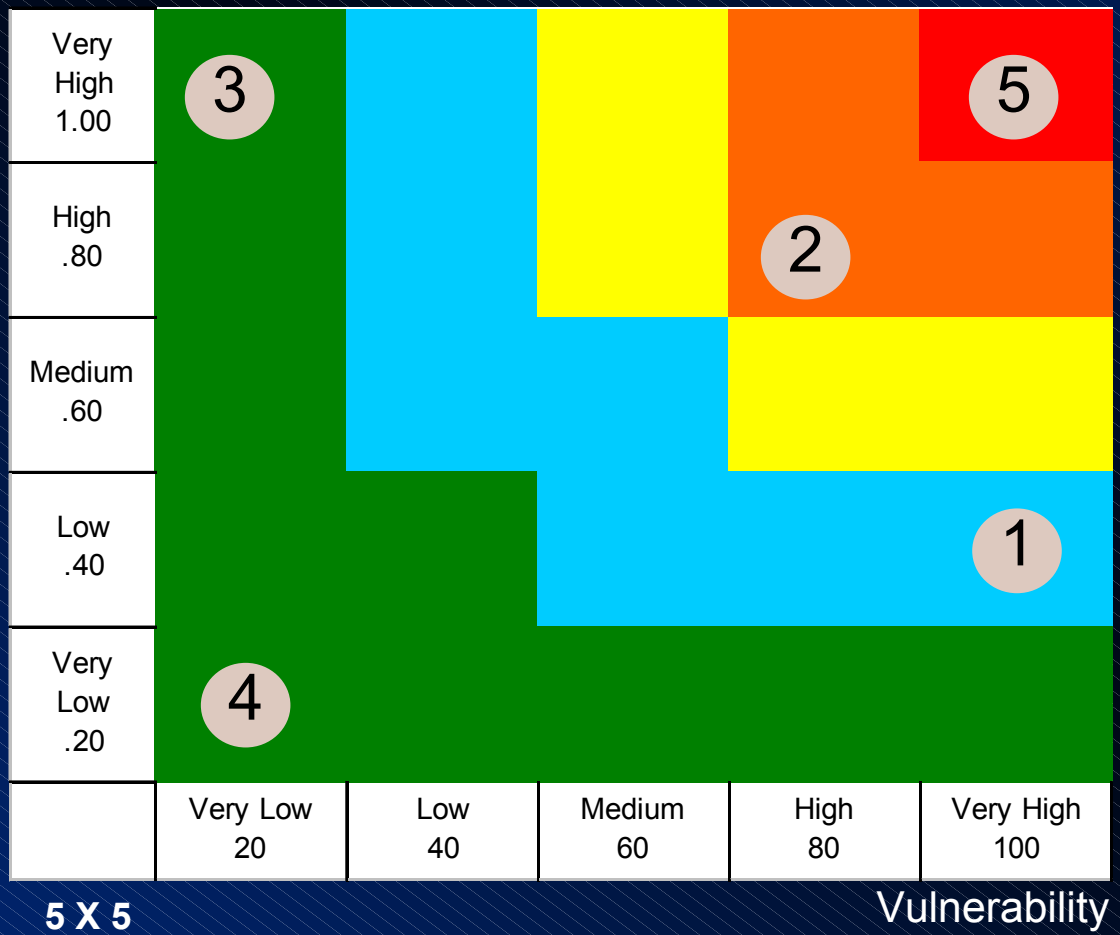


5 X 5
Very Low 1 to 20 (40%)
Low >20 to 40 (28%)
Med >40 to 60 (16%)
High >60 to 80 (12%)
Very High >80 to 100 (4%)



4 X 4
Negligible 1 to 25 (50%)
Low >25 to 50 (31%)
Med >50 to 75 (13%)
High >75 to 100 (6%)

Risk Plotting



5 X 5

Very Low	1 to 20
Low	>20 to 40
Med	>40 to 60
High	>60 to 80
Very High	>80 to 100

Item 1		
Unauthorized Access to Servers		
Vulnerability	Very High	100
Threat	Low	0.40
Value		40.00

Item 2		
Password Security Practices by Workforce		
Vulnerability	High	80
Threat	High	0.80
Value		64.00

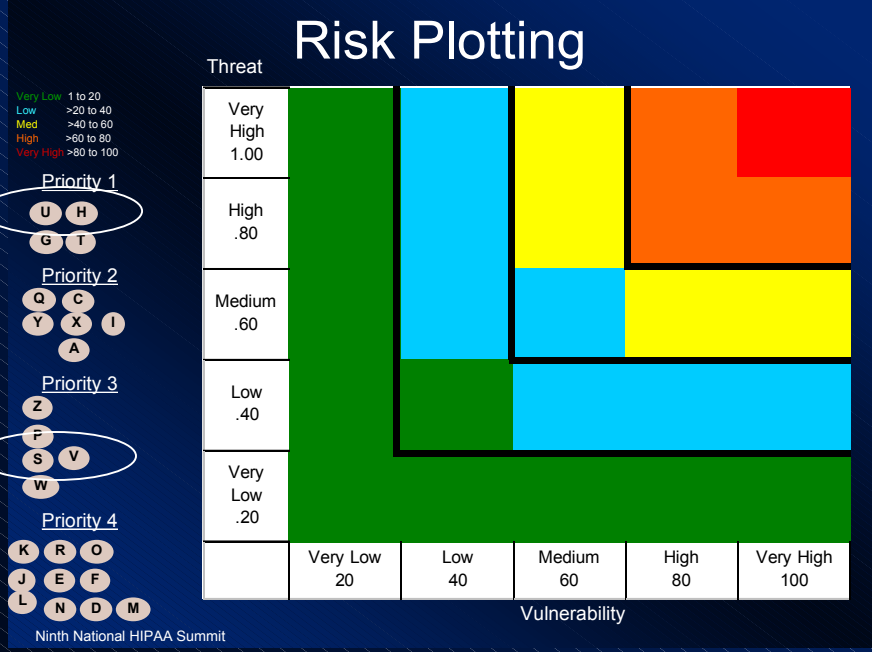
Item 3		
User Intoduced Virus (Non-email)		
Vulnerability	Very Low	20
Threat	Very High	1.00
Value		20.00

Item 5		
Data Pirating		
Vulnerability	Very High	100
Threat	Very High	1.00
Value		100.00

Item 4		
Weather Induced Flood		
Vulnerability	Very Low	20
Threat	Very Low	0.20
Value		4.00

Tie Breakers

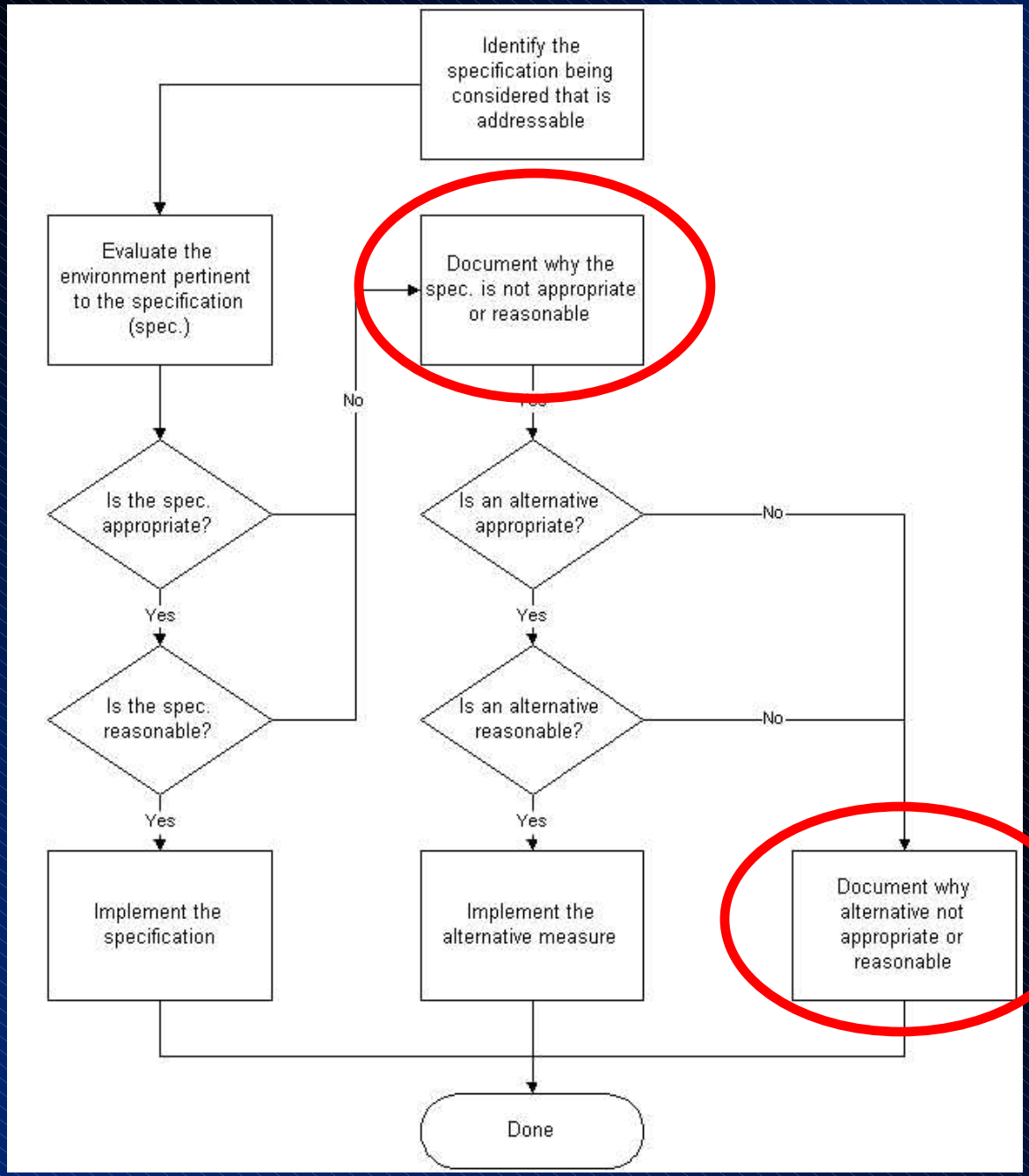
- Cost
  - $ of loss
  - $ to replace
  - $ recover



(Risk Plot Value) * Cost = Expected Cost

Helpful Hint:
Make use of available cost data.

Addressable Review Flow



- Consistent approach
- Documentation points
- Dynamic

Helpful Hint: Involve different departments.

Summary:

- Define and apply terms
- Identify level of risk aversion
- Gather information
- Quantify and compare threat-vulnerability risk plots
- Identify required and addressable specifications
- Document either by policy or in position statement

"There is a time for daring and a time for caution, and a wise man knows which is called for."

John Keating, Teacher in Dead Poet's Society