The Foundations of Risk Management:

6 May 1997

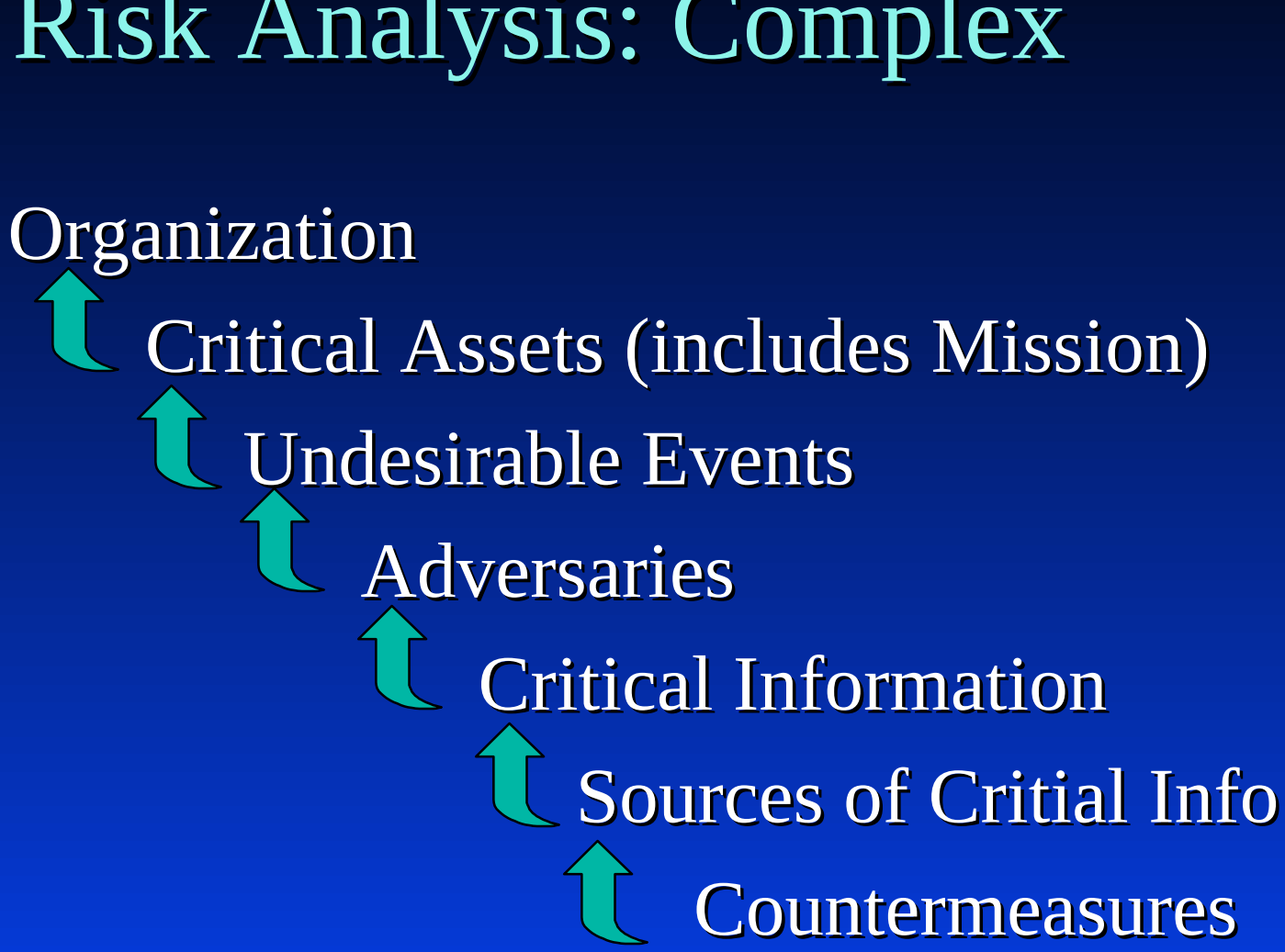
NSA's INFO SYSTEMS SECURITY Customer Services Support (V1)

Dr. Donald R. Peeples

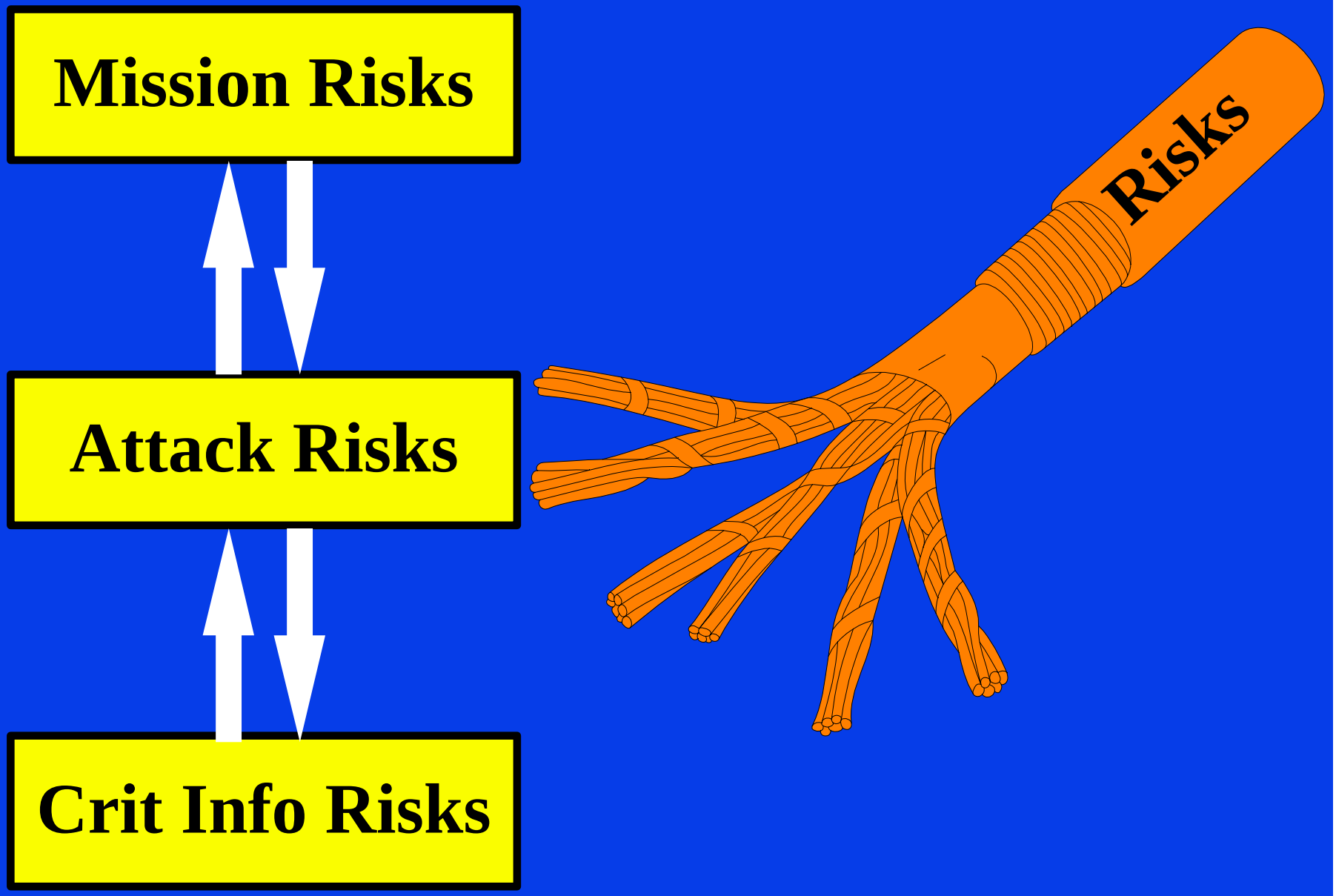
Risk Analysis: Complex

- Organization
  - Critical Assets (includes Mission)
    - Undesirable Events
      - Adversaries
        - Critical Information
          - Sources of Critial Info
            - Countermeasures

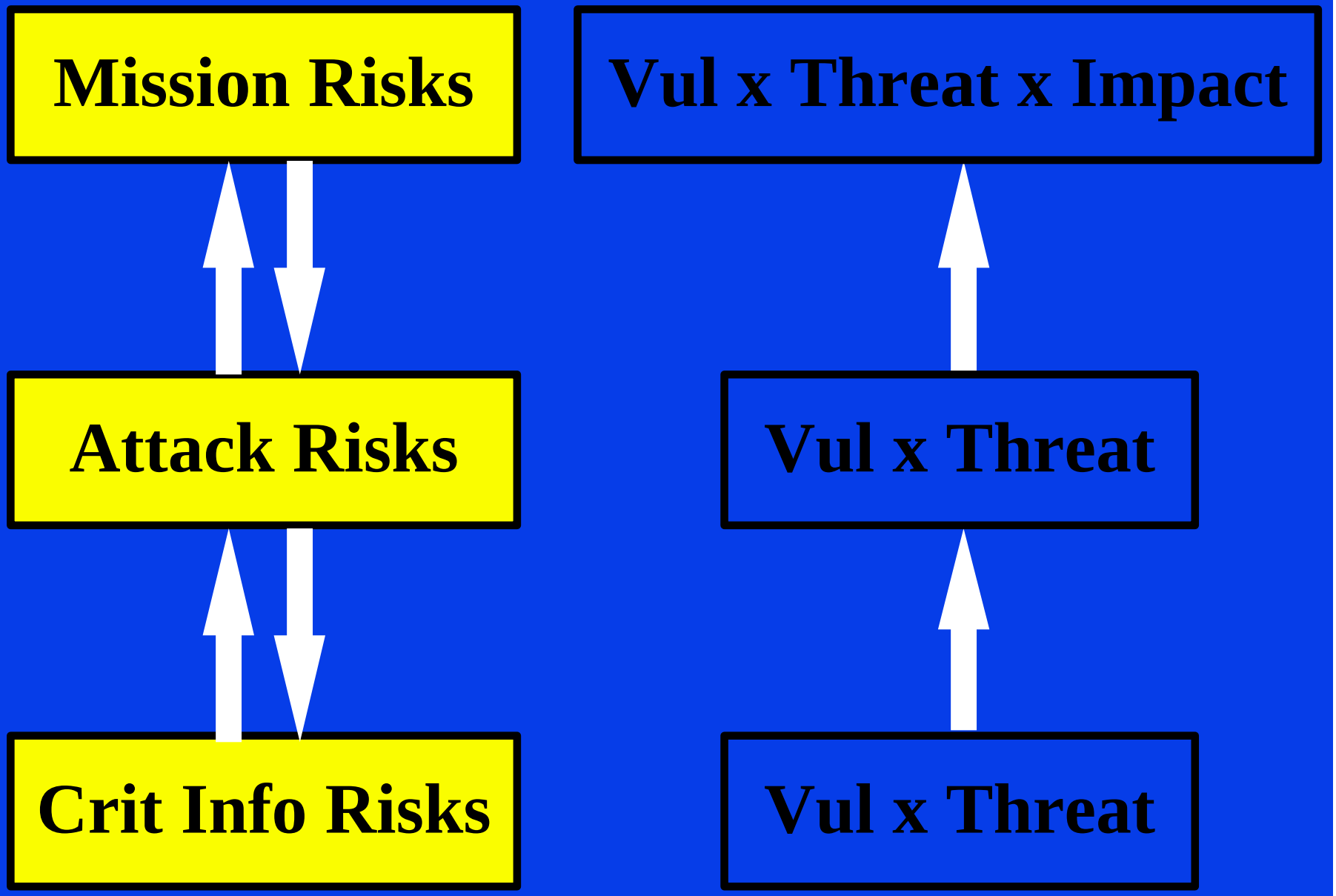
Risk Analysis: Complex



Risk Analysis: Three Levels

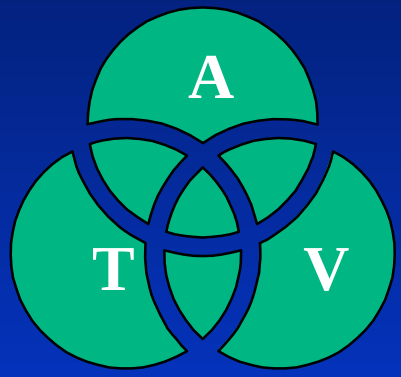


Risk Analysis: Three Levels



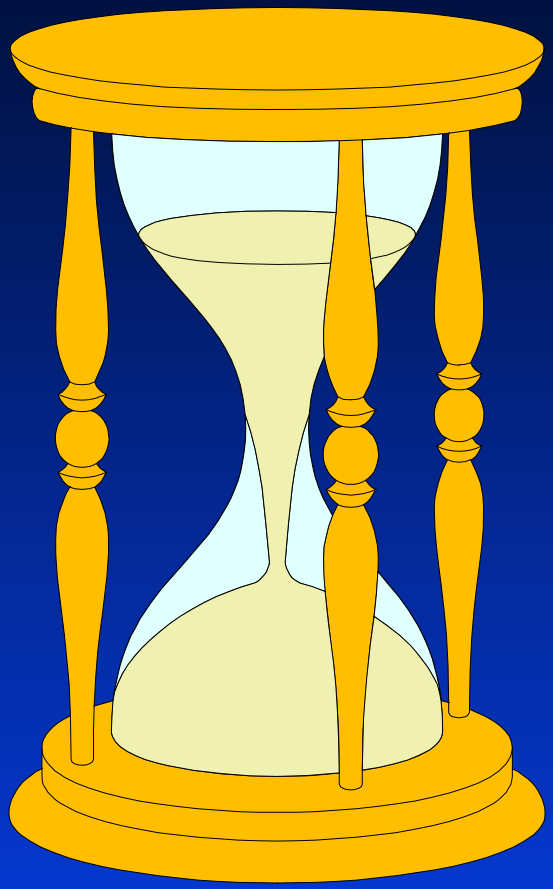
Goals

- Given: Sets of Countermeasures
  - How to Decide Which is Better
- Aggregate:
  - Asset Replacement Value
  - Measure of Threat
  - Measure of Vulnerability



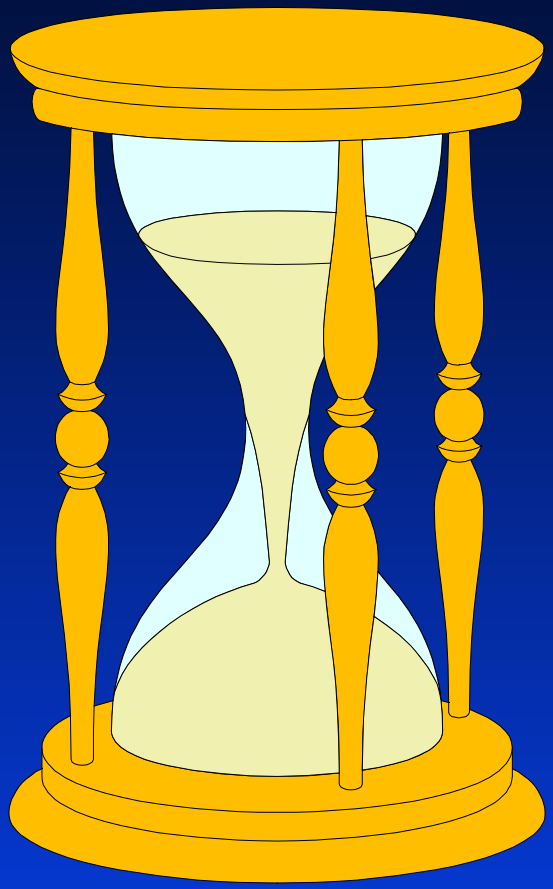
Agenda

- First Principles of Risk Management
- Countermeasures (Benefit/Cost)
- Data Types
- Risk Analysis Data Aggregation
- VISART Details

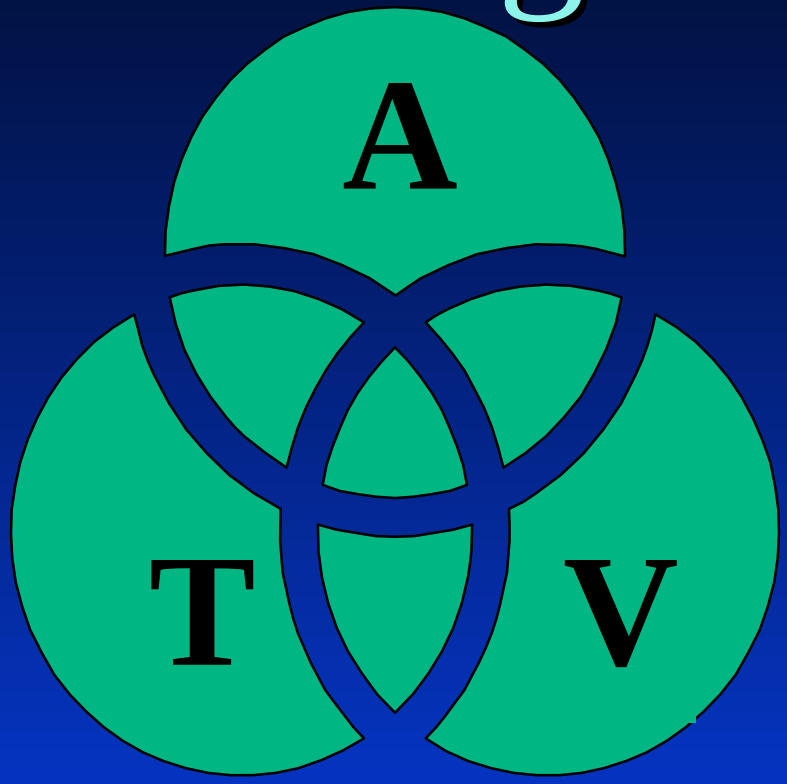


Agenda

- First Principles of Risk Management
- Countermeasures (Benefit/Cost)
- Data Types
- Risk Analysis Data Aggregation
- VISART Details



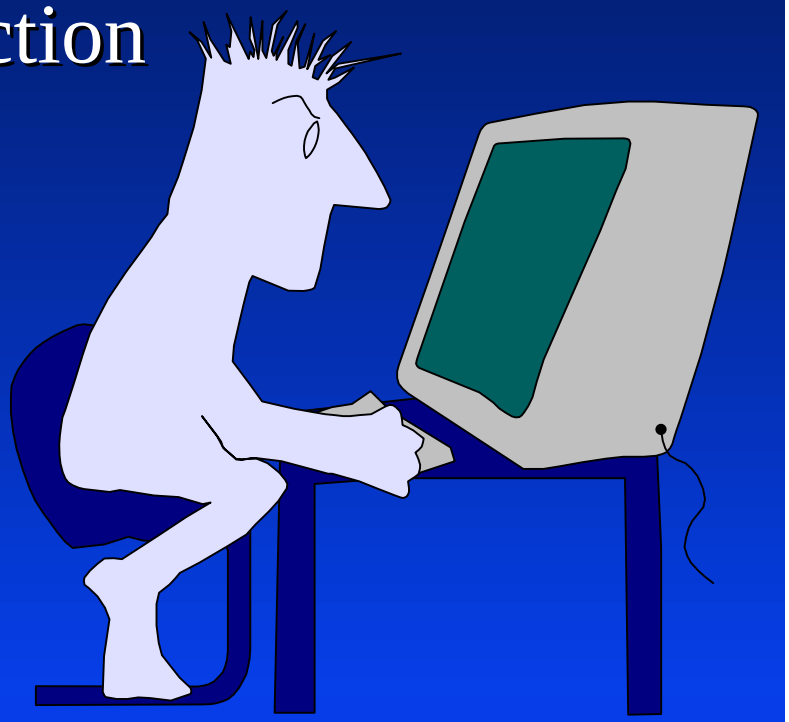
Risk Management:



First Principles

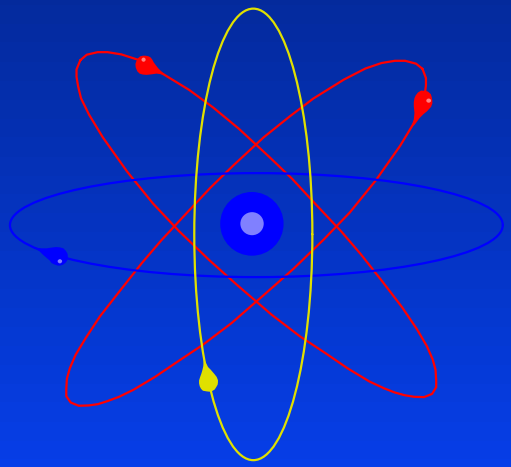
Undesirable Event:

- One that Harms or Damages One's Assets
  Directly
  Not Information Collection

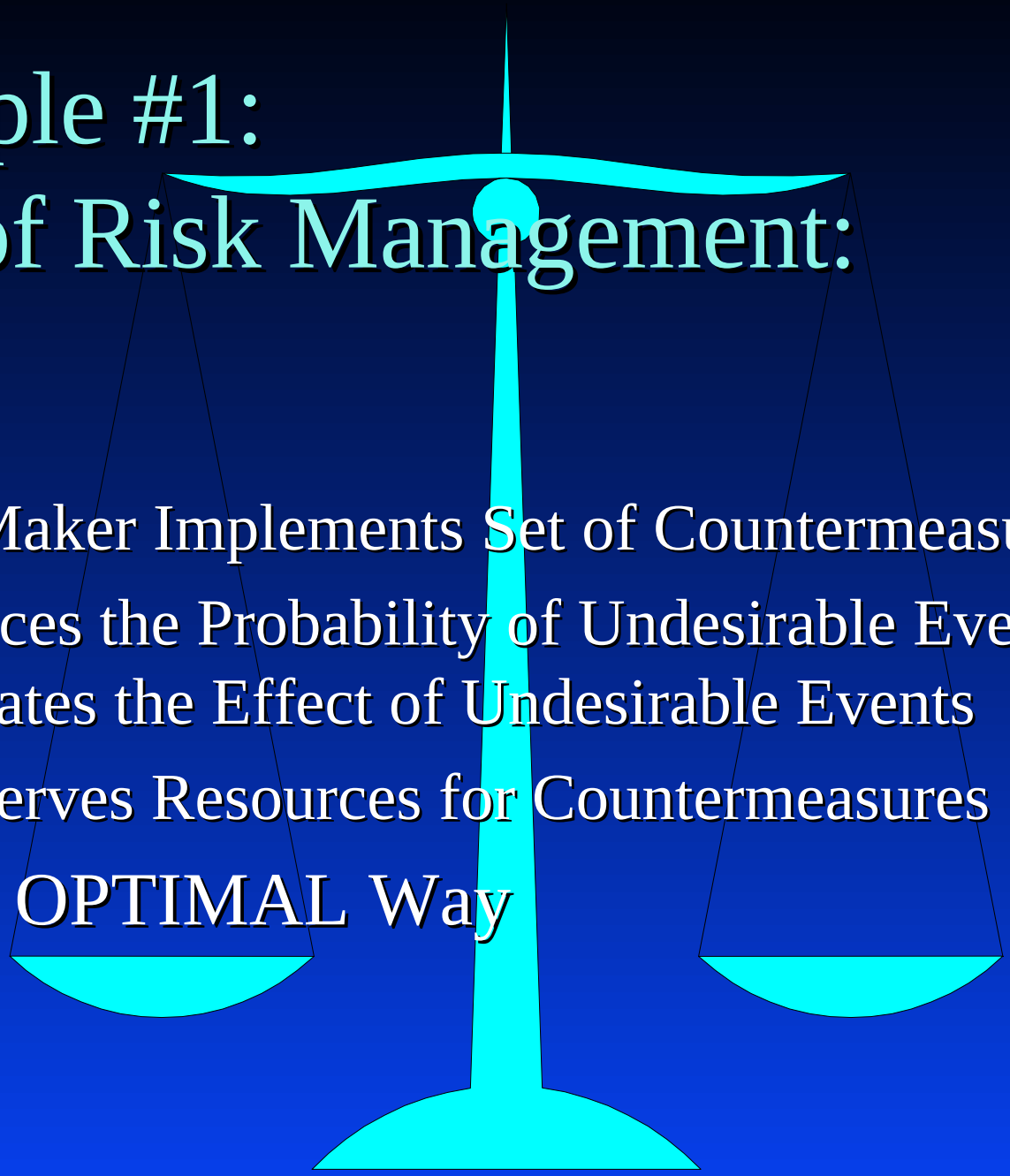


Scope of Risk Management

- Health
- Safety
- Theft of Property
- Security
  - Security of Information
    - Confidentiality
    - Integrity
    - Availability
    - Non-Repudiation



Principle #1: Goal of Risk Management:



Decision Maker Implements Set of Countermeasures

- Reduces the Probability of Undesirable Events or Mitigates the Effect of Undesirable Events
- Conserves Resources for Countermeasures
- In an OPTIMAL Way

Expected Value

- GAME
  - Flip Coin 100 times
  - If Heads: Win $1.00
  - If Tails: Win $2.00

COIN TOSS (Head $1; Tail $2)

- Question: What is Maximum Winning for the 100 Tosses? How?
- Question: What is Minimum Winning for the 100 Tosses? How?
- Question: What are Expected Winnings for the 100 Tosses?
- Question: What are Expected Winnings per Toss for the 100 Tosses?

Expected Payoff

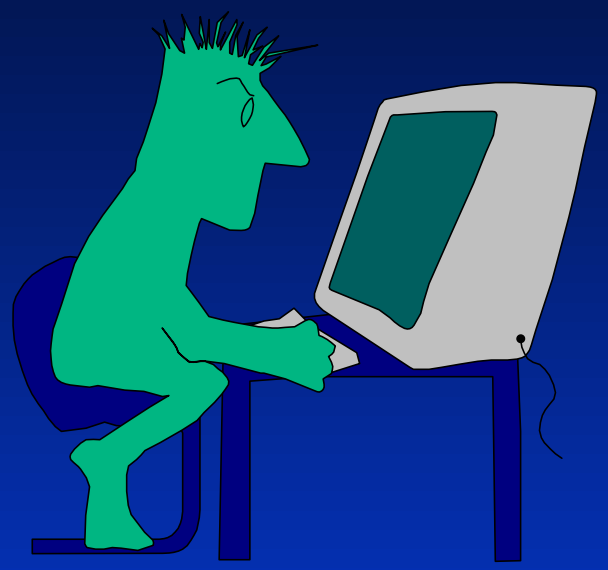
- Heads
  - 1/2 x $1.00 = $.50 (PROB x PAYOFF)
- Tails
  - 1/2 x $2.00 = $1.00 (PROB x PAYOFF)
- Total
  - $.50 + $1.00 = $1.50 (ADD)

Expected (Value) Payoff

- Question: What is Most You Pay for One Toss?
- Question: What is Least the “House” Would Want You Pay for One Toss?
- $1.50, called the “FAIR PRICE” of Game
- MOST YOU WANT TO PAY!

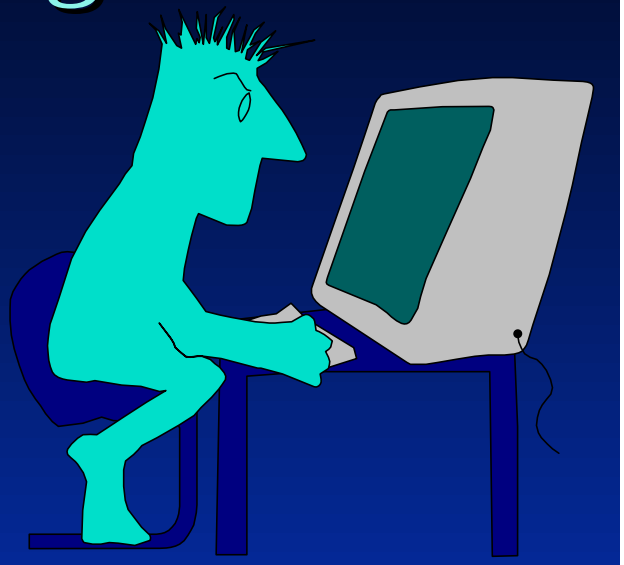
Principle #2: Measuring RISK

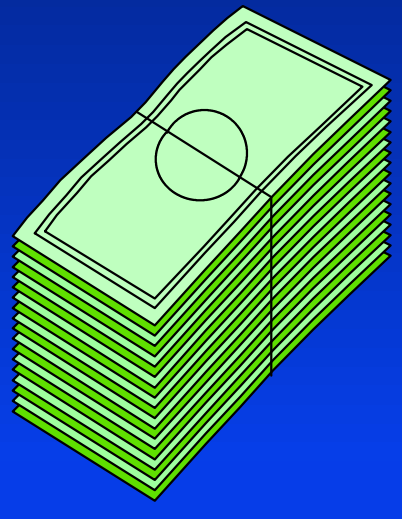
- Undesirable Event has:
  - Probability of Occurrence
  - Impact to Organization
- The Measure of RISK is:
  - Expected Impact =
  - Probability x Impact



Principle #2: Measuring RISK

- Undesirable Event has:
  - Probability of Occurrence
  - Impact to Organization
- The Measure of RISK is:
  - Expected Impact =
  - Probability x Impact
- MOST YOU WANT TO PAY FOR PROTECTION!





Principle #3: Probability of Occurrence

- Threat Capability and Motivation (*)
  - Adversaries (*)
  - Natural Hazards
  - Random Human Error

- Vulnerability -- Weakness in Protection System
- How to Combine When Measuring
- MULTIPLY!

Scenario

- Threat has 60% Chance of Having Motivation & Capability to Attempt a State-of-the-Art Attack [THR = .60]
- Our Safeguards Protection System CANNOT Protect our Assets from exactly 40% of State-of-the-Art Attacks [VUL = .40]
- What is Probability of a Successful Threat Attack?

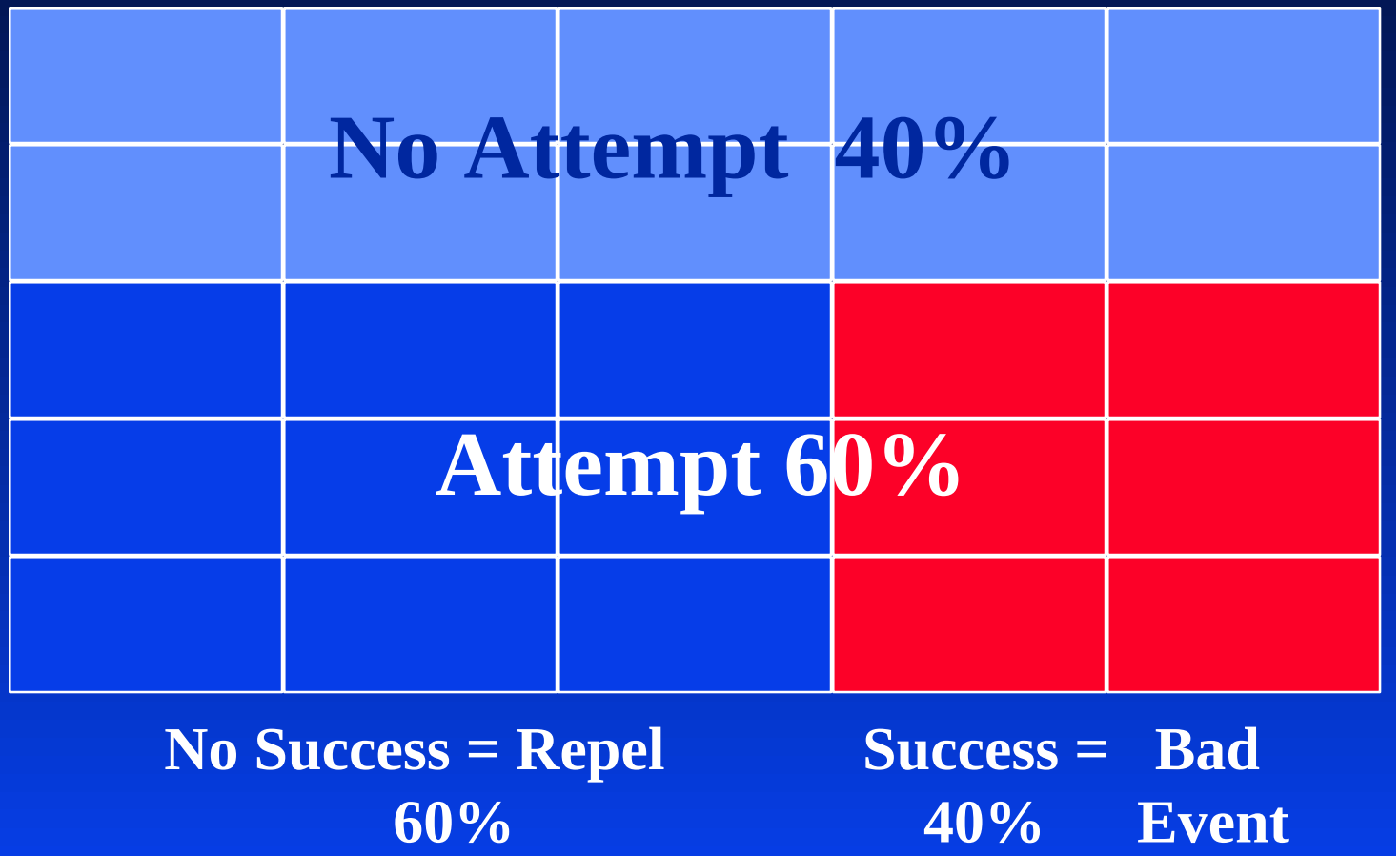
Threat Attempt

	No Attempt 40%			
	Attempt 60%			

Scenario

Our Safeguards Protection System
CANNOT Protect our Assets from
exactly 40% of State-of-the-Art Attacks
[VUL = .40]

Successful Threat Attack



Successful Threat Attack

- 6/25 = 24/100 = .24
- Also, .60 x .40 = .24
- Multiplication of Threat and Vulnerability Measures
- Always Works to Multiply!

Summary: First Principles of RM

- Decision Maker Implements a Set of Countermeasures:

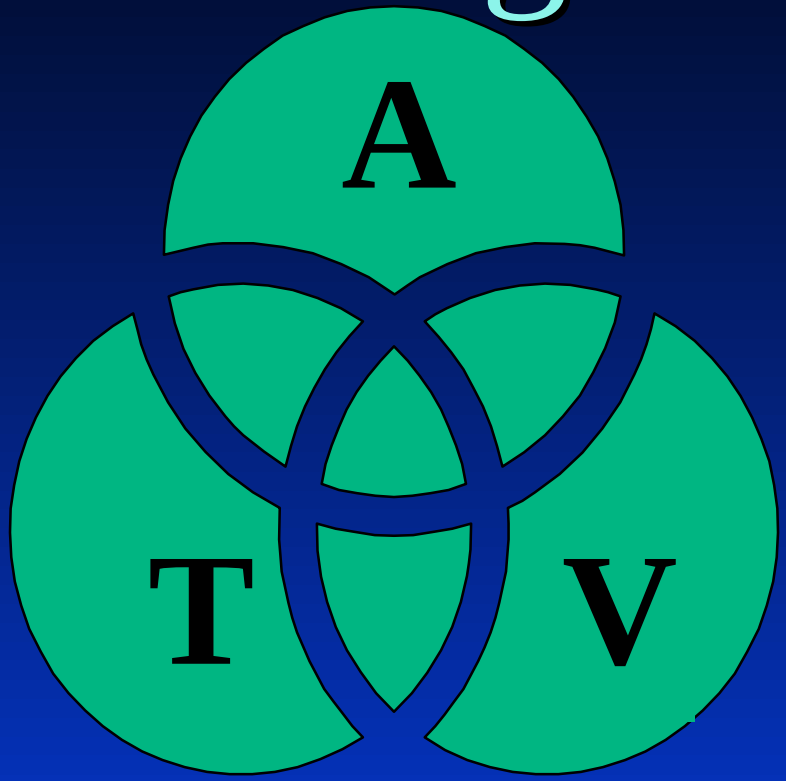
  Reduces the RISKS of Undesirable Events

RISK =
VULNERABILITY x THREAT x IMPACT

  Conserves Resources for Countermeasures

  In an OPTIMAL Way

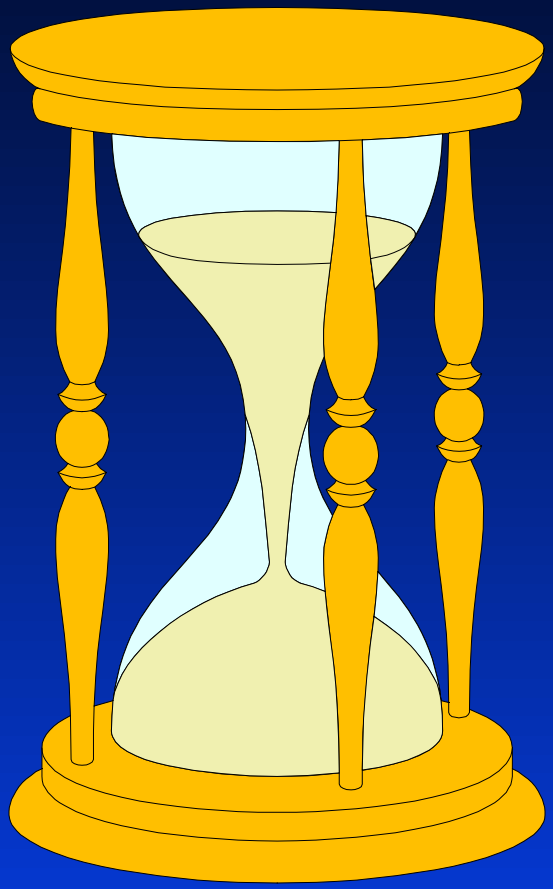
Risk Management:



First Principles

Agenda

- First Principles of Risk Management
- Countermeasures (Benefit/Cost)
- Data Types
- Risk Analysis Data Aggregation
- VISART Details



Countermeasures (Benefit/Cost)

- Coin Toss:
- Friend Offers Weighted Coin
- Prob[Tails] = .75
- House will Allow Use but
- Costs extra $.10
- Is Weighted Coin Worthwhile?

Is Weighted Coin Worthwhile?

Expected Payoff

$1.75

.25 x 1.00 + .75 x 2.00

Benefit

$.25

1.75 - 1.50

Cost

$.10

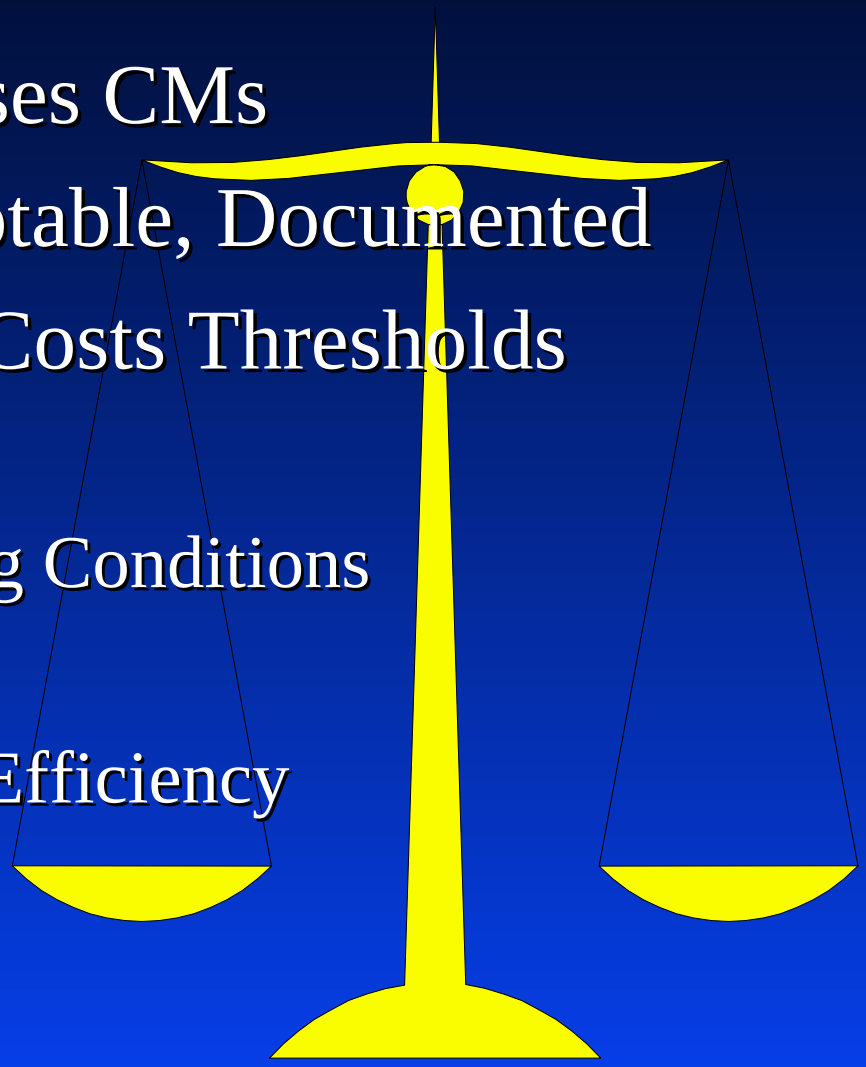
Net Benefit

$.15

.25 - .10

Why Risk is Important to RM

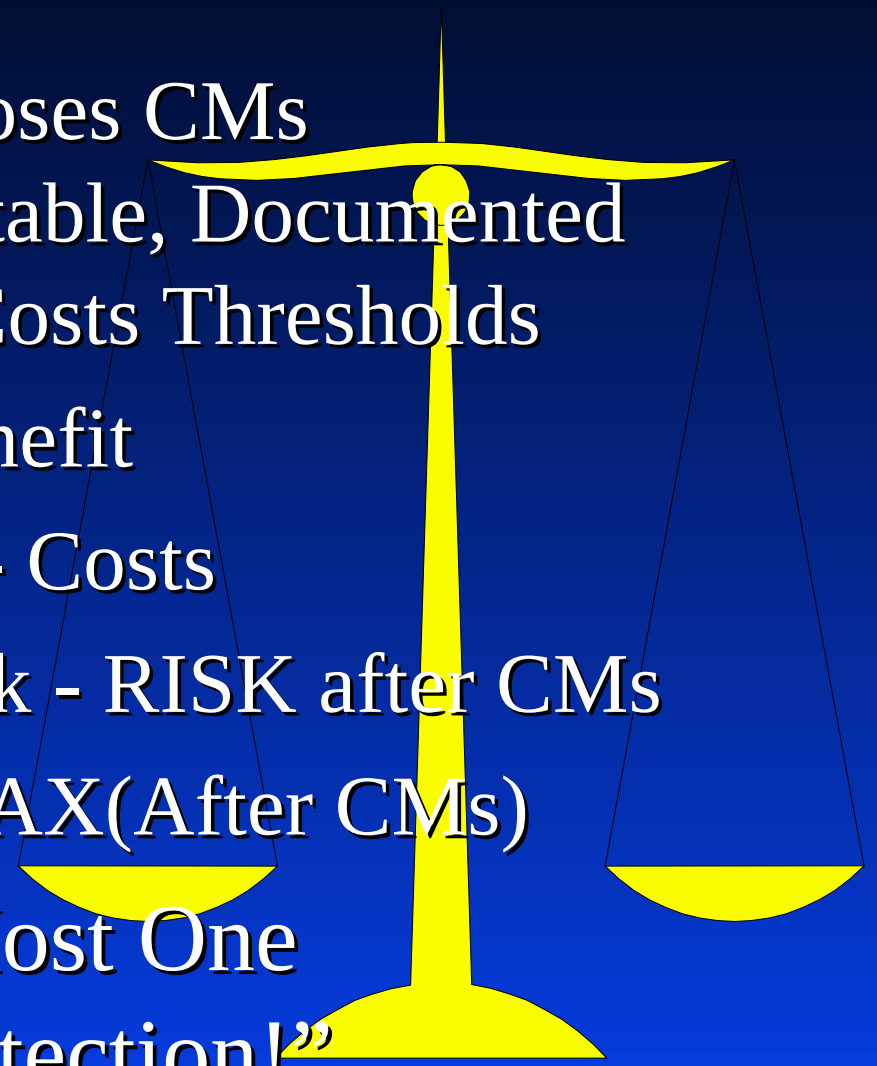
- Risk Manager Chooses CMs
- Criteria: Best, Acceptable, Documented
- Acceptable: Within Costs Thresholds
  - Dollars
  - Unfavorable Working Conditions
  - Political Fallout
  - Loss of Operational Efficiency
  - Loss of Reputation



Why Risk is Important to RM

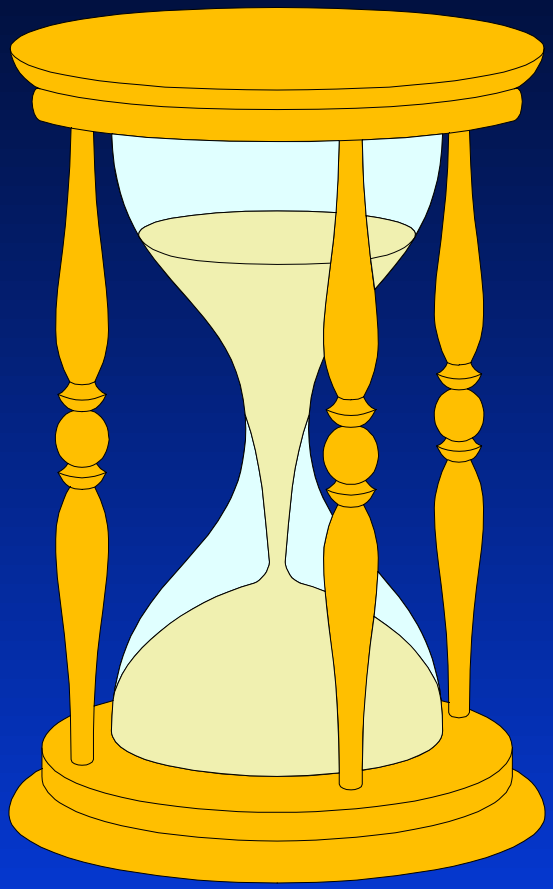
- Decision Maker Chooses CMs
  Criteria: Best, Acceptable, Documented
  Acceptable: Within Costs Thresholds
- Best: Largest Net Benefit
- Net Benefit: Benefit - Costs
- Benefit: Baseline Risk - RISK after CMs
- MAX (Baseline) - MAX(After CMs)

"Reduction in the Most One Should Pay for Protection!"



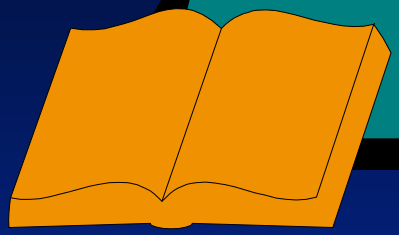
Agenda

- First Principles of Risk Management
- Countermeasures (Benefit/Cost)
- Data Types
- Risk Analysis Data Aggregation
- VISART Details



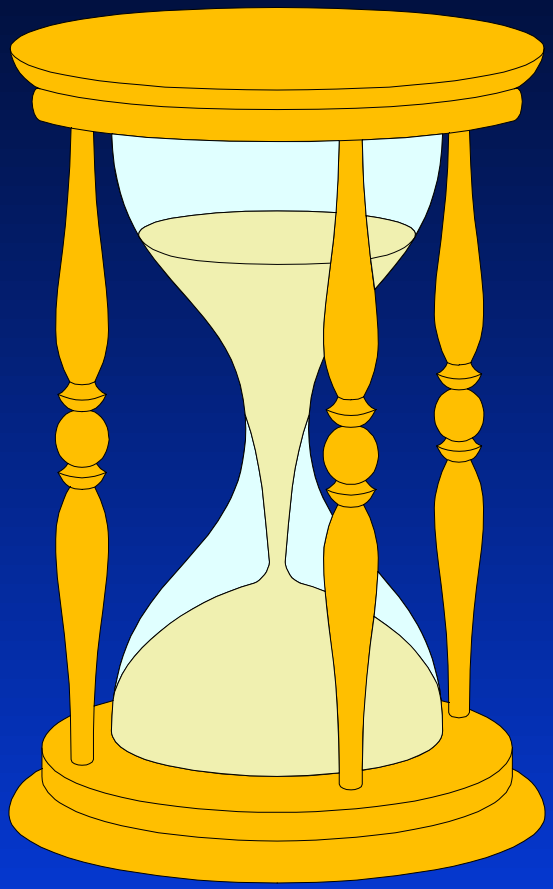
D Types

- itative v uantitative
  - ISART F ble
  - uantitat
    - Linguistic: LO, MED, HI
    - Numerical: 91
- Quantitative Granularity
  - {LO, HI}
  - {LO, MED, HI, CRIT}
  - {VLO, LO, MLO, MED, MHI, HI, VHI}
  - {1, 2, 3, ... , 100}
  - All positive numbers.

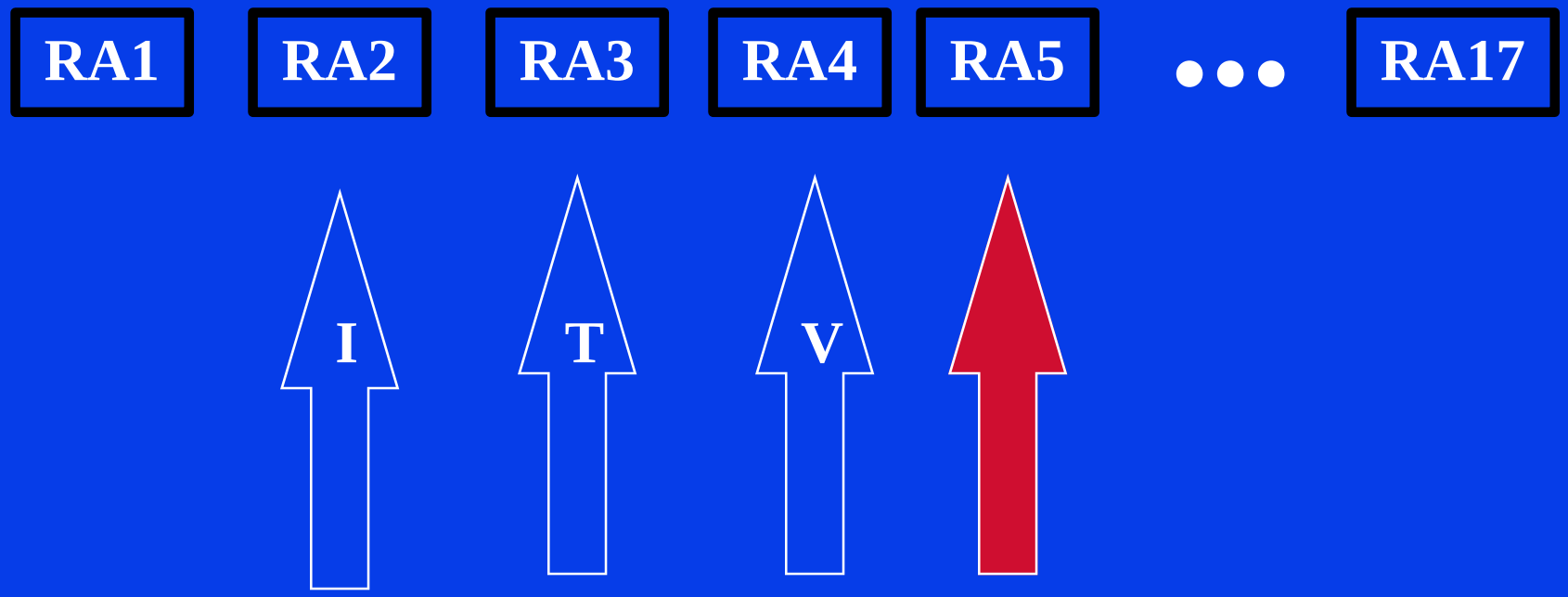


Agenda

- First Principles of Risk Management
- Countermeasures (Benefit/Cost)
- Data Types
- Risk Analysis Data Aggregation
- VISART Details



Risk Analysis Process



{ LO, MED, HI, CRIT }

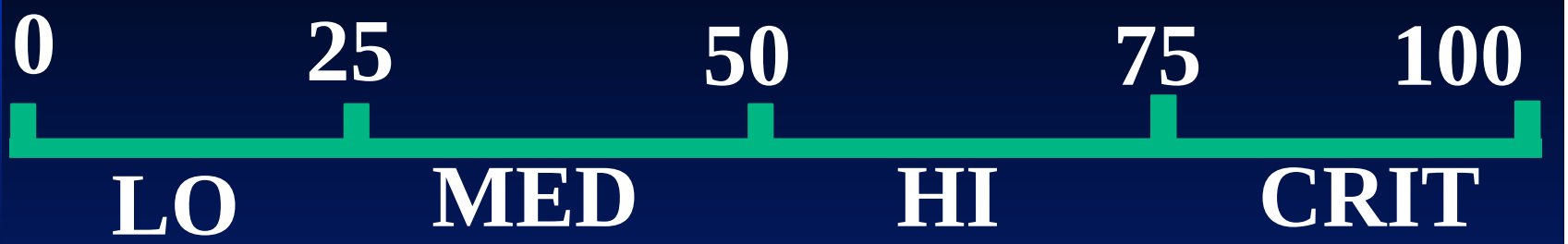
Plan of Attack -- STRUCTURED!

- Start with I, T, V Linguistics
- Convert {LO, MED, HI, CRIT} to Numbers
- Multiply Three Numbers for RISK
- Reconvert to {LO, MED, HI, CRIT}

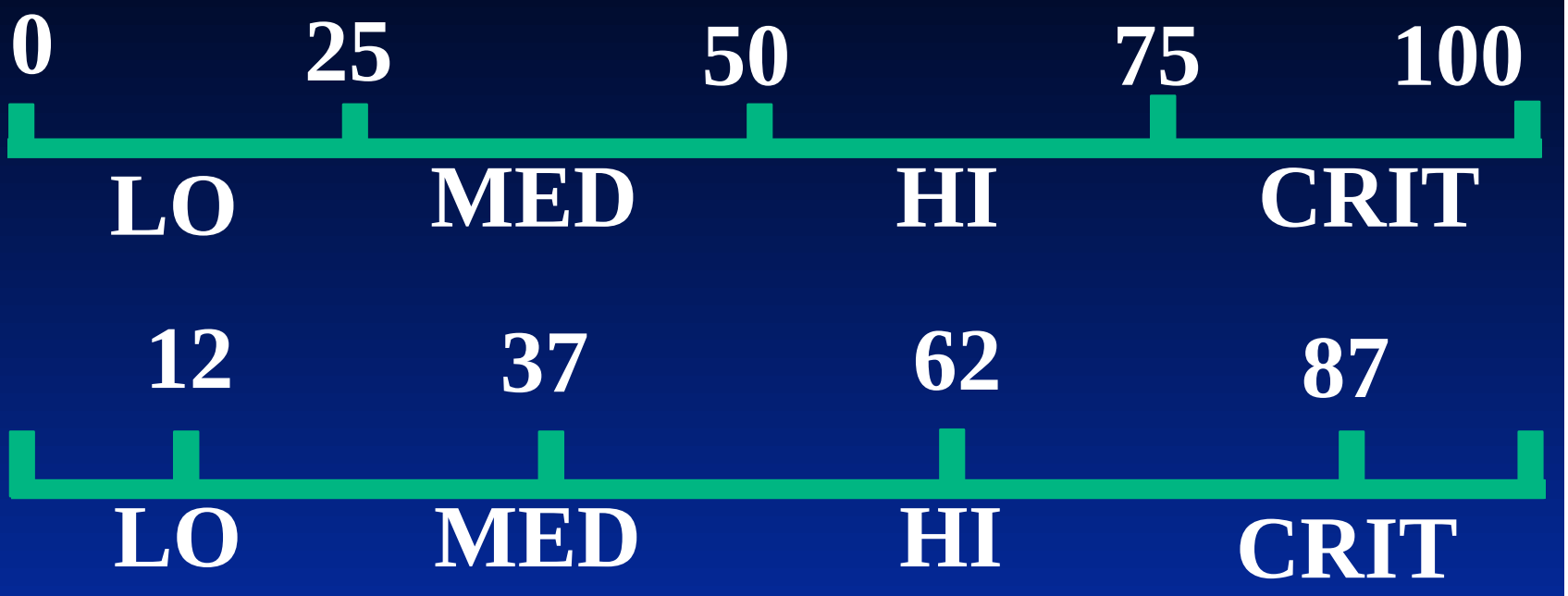
Choice of Scale

- What Does “Critical” Mean?
- Mind of the Decision Maker/Risk Manager!

One Way



One Way



- 87/12 = 7 [approximately]
- IMPACT: Do Seven “LO’s” Equal One “Critical”?
- Why Not Use Numbers Initially?

Suggested Scaling

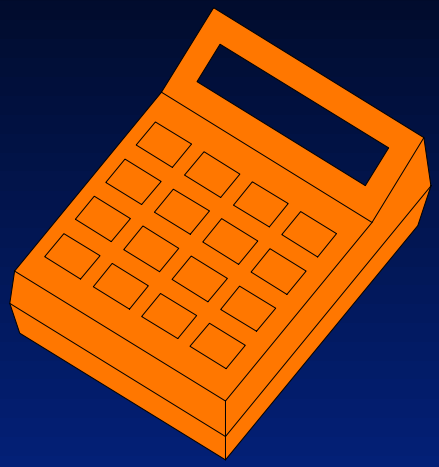
Impact & Risk

	Low	Medium	High	Critical
Value	.1	1	10	100
Range	0 - .3	.3 - 3	3 - 30	30 - 100
Example	Haiti	Somalia	Desert Storm	Nuclear War

Threat & Vulnerability

	Low	Medium	High	Critical
Value	12	37	62	87
Range	0 - 25	25 - 50	50 - 75	75 - 100

Aggregation

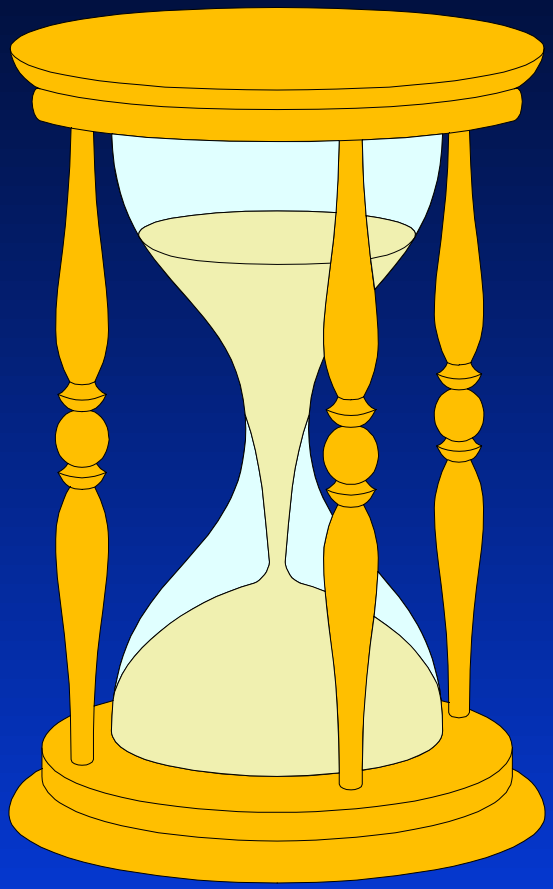


- THREAT = MLO
- VUL = HI
- IMPACT = HI

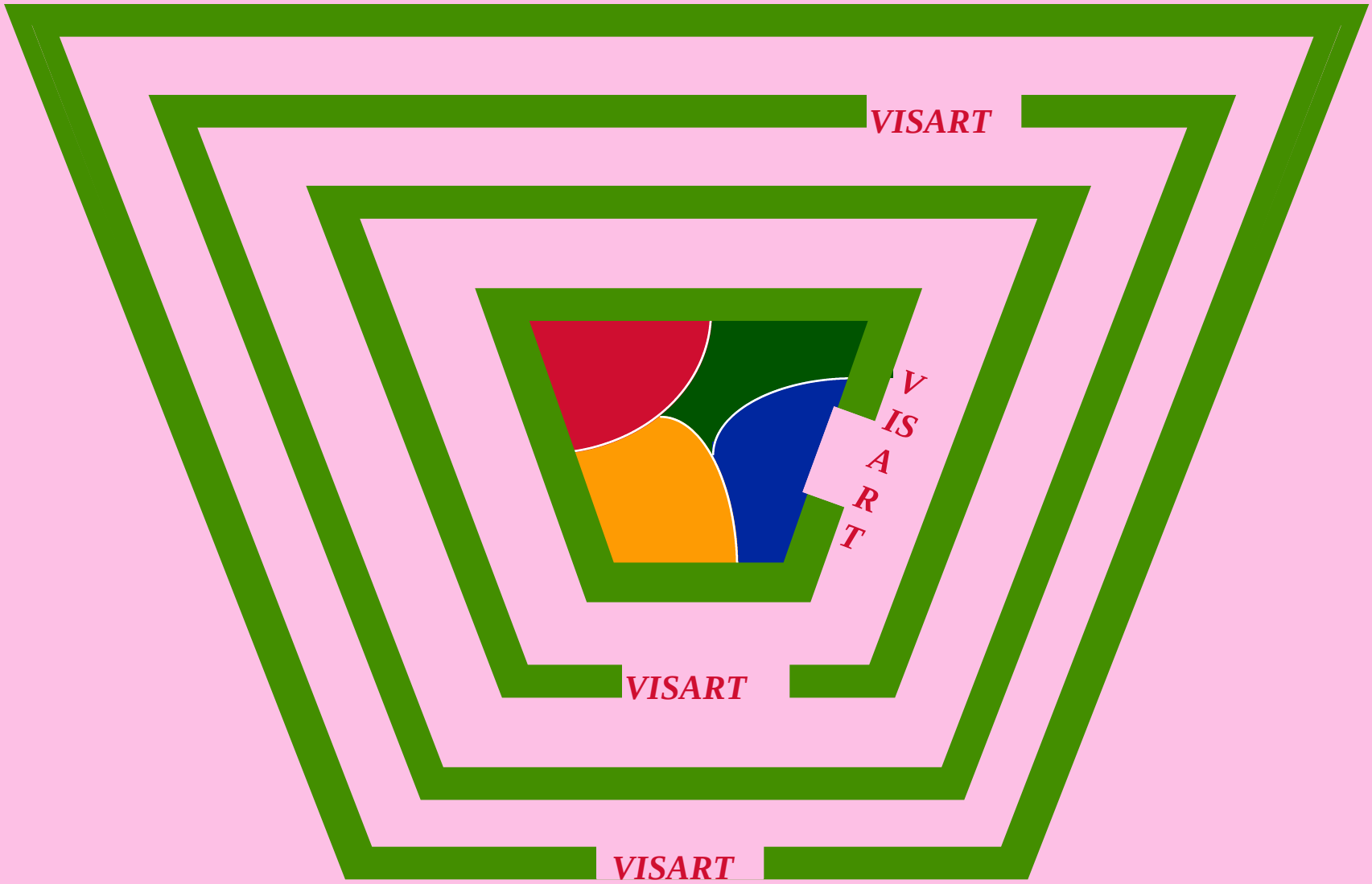
- THREAT = .25
- VUL = .62
- IMPACT = 10
- RISK = 1.55 or MED

Agenda

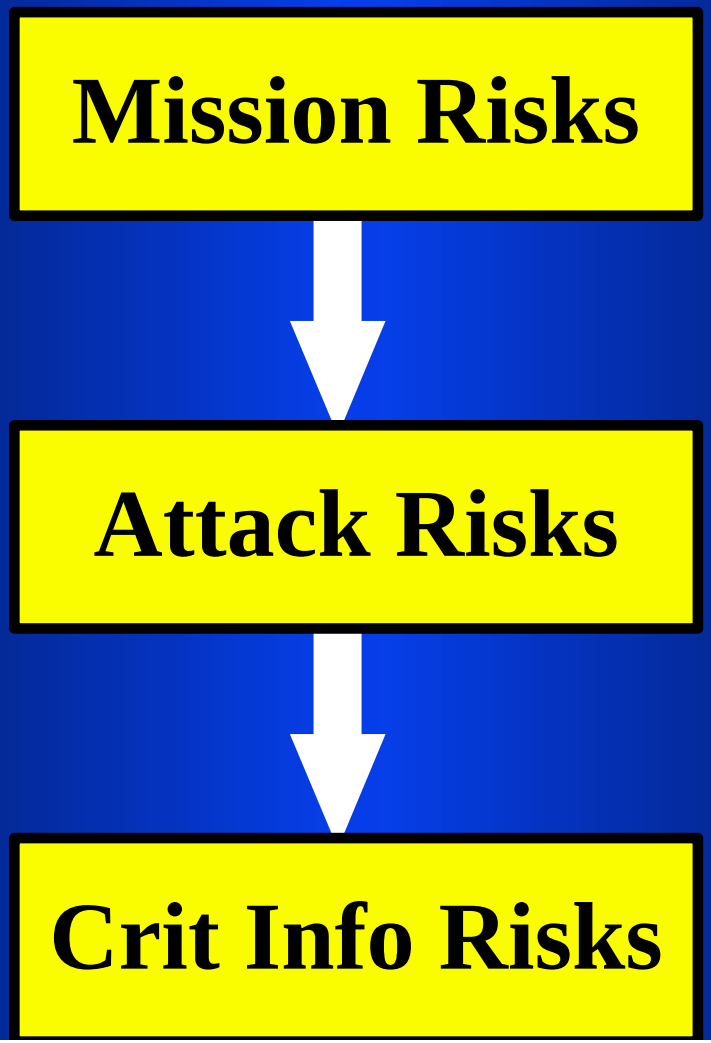
- First Principles of Risk Management
- Countermeasures (Benefit/Cost)
- Data Types
- Risk Analysis Data Aggregation
- VISART Details

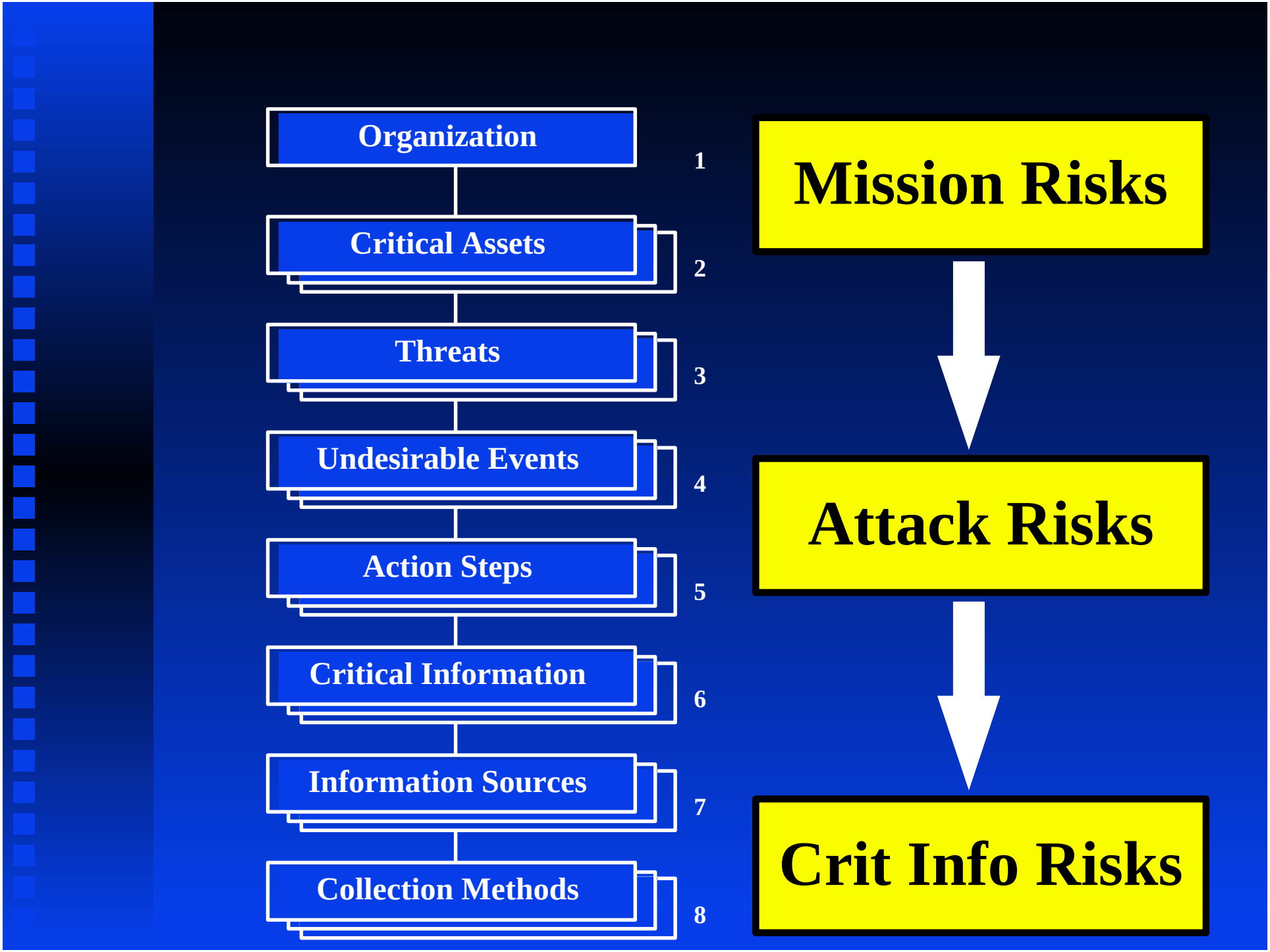


VISART

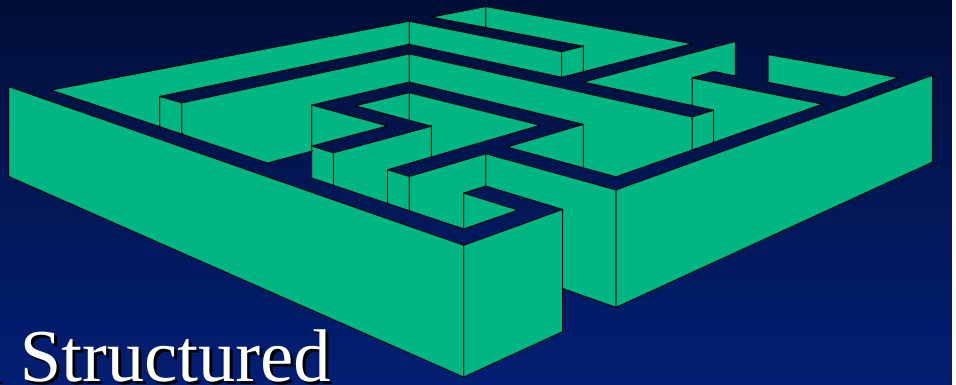


Risk Analysis: Three Times



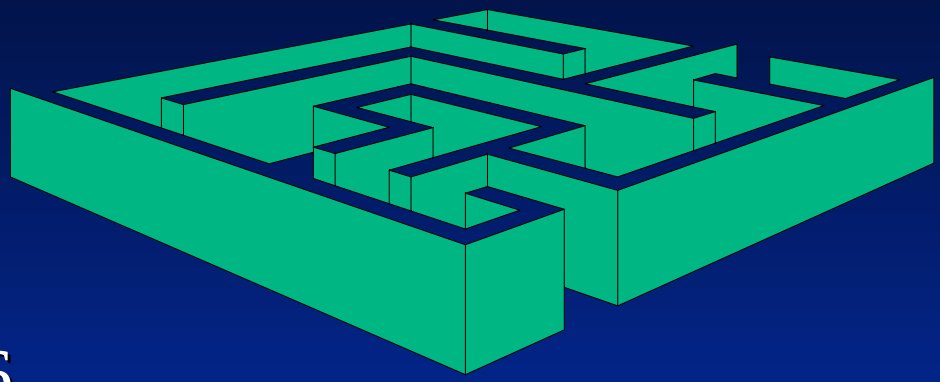

Organization
1
Critical Assets
2
Threats
3
Undesirable Events
4
Action Steps
5
Critical Information
6
Information Sources
7
Collection Methods
8
Mission Risks
Attack Risks
Crit Info Risks

VISART



- Value of Information Structured Analysis of Risk Tool
- Risk Analysis Data Management Software
- PC & Windows 3.1 (Laptop)
- Applies to ANY Protection Situation
- Guide to a Thought Process
- No Questionnaires
- Beginning, End, No Middle

VISART
Status



- Delivered 1 OCT 96
- Classes 1997
- Software ONLY at End of Class (?)

The Foundations of Risk Management:

6 May 1997 **NSA/V1**

Dr. Donald R. Peeples (410) 859-4737