Information Assurance Metrics Highlights

Dr. Michael Schildcrout

Naval Security Group

Outline

- **Metrics Development Process**
  - **Joint Service Effort**
  - **DOT&E Sponsorship**
- **Risk Levels**
- **Remaining Issues**

Information Assurance Metrics for Operational Test & Evaluation

- **Metrics for IA OT&E must be:**
  - **Physically observable**
  - **Measurable**
  - **Quantitative, when feasible**
- **Directly related to overall goal:**

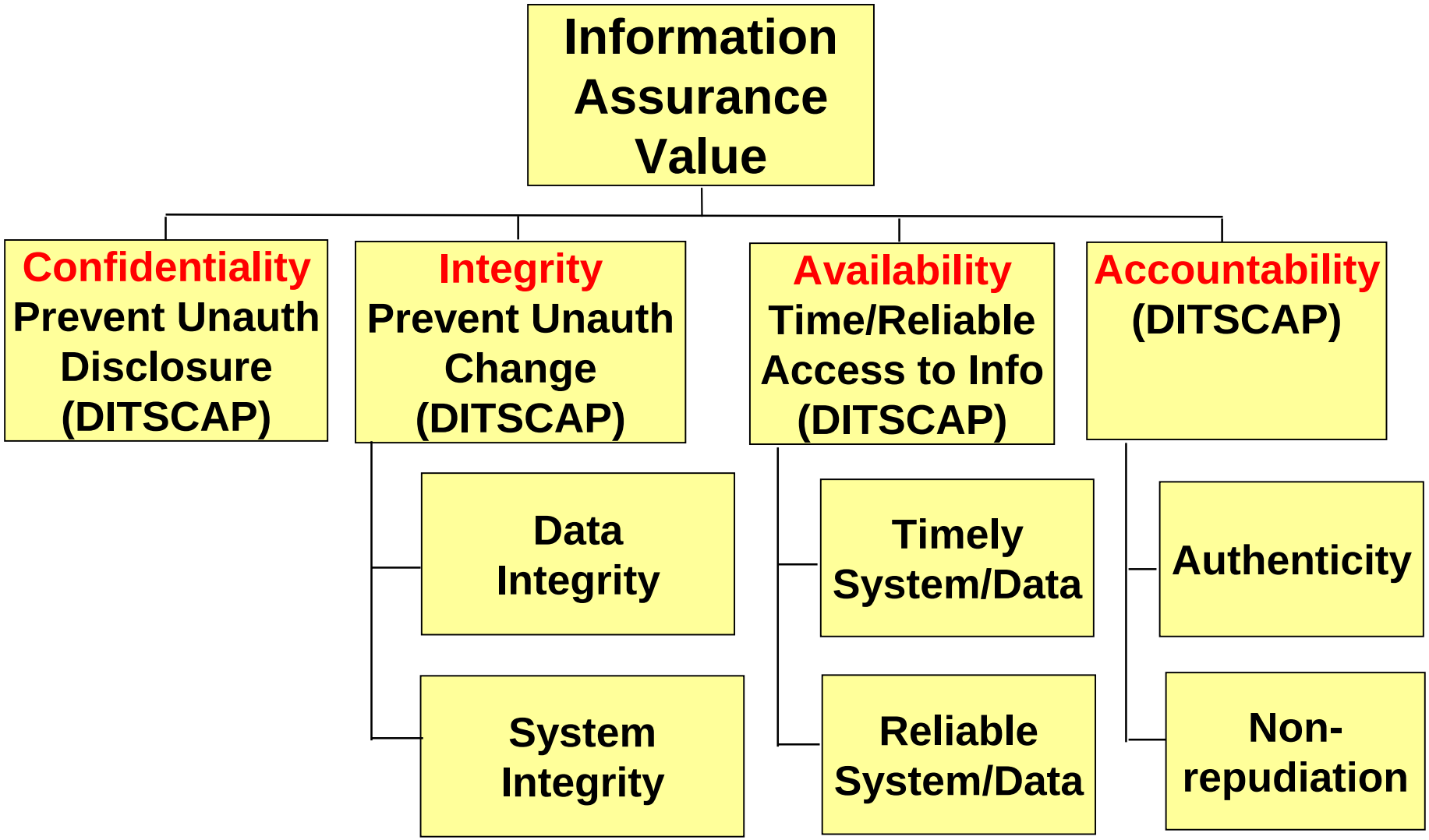
Protection of Information

DITSCAP

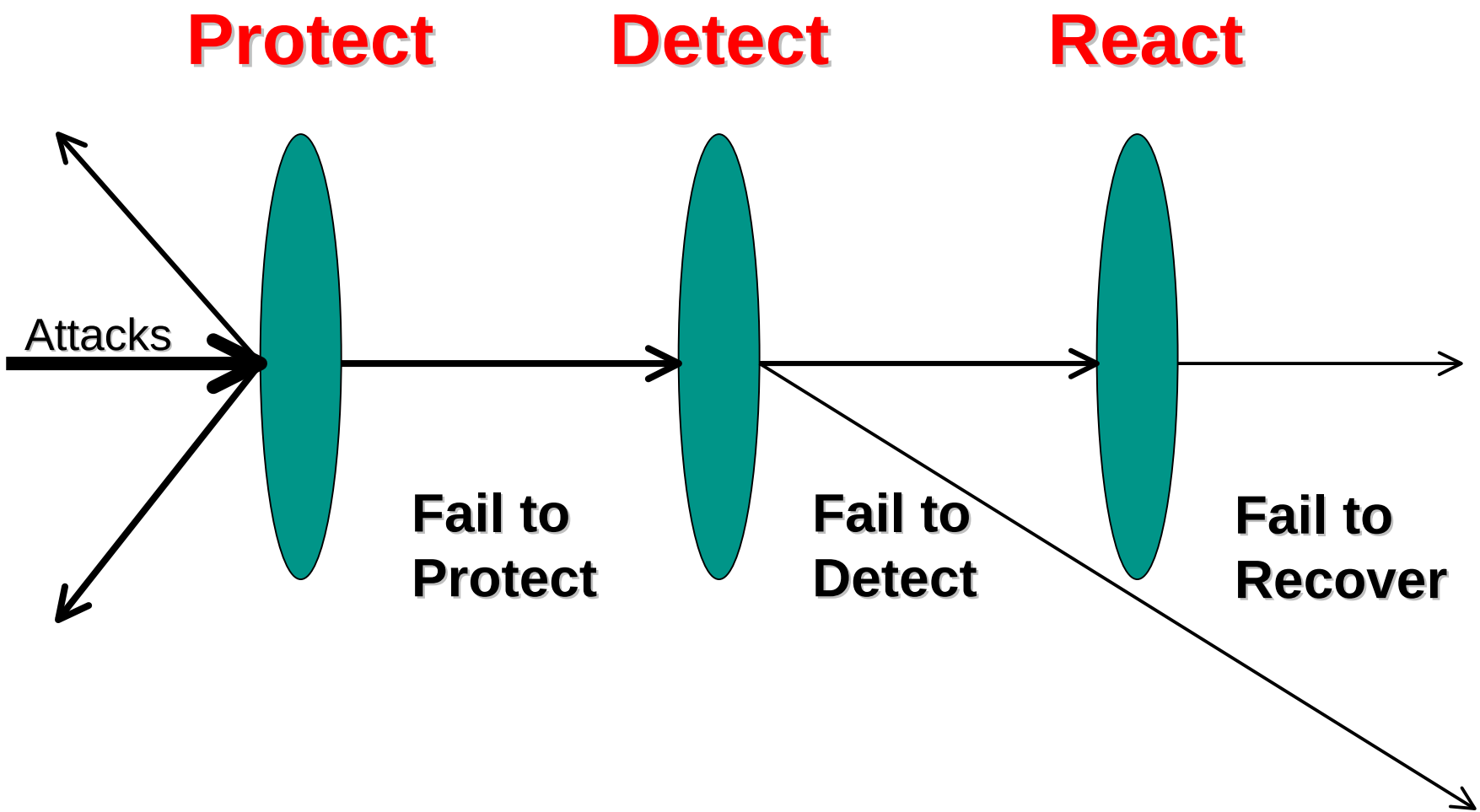
DoD Information Technology Security Certification and Accreditation Process

- Developed by the DT Community
- Four Phases. Each phase contains a stage of vulnerability assessment
  - Phase 1: Definition
  - Phase 2: Verification
  - Phase 3: Validation
  - Phase 4: Post-Accreditation

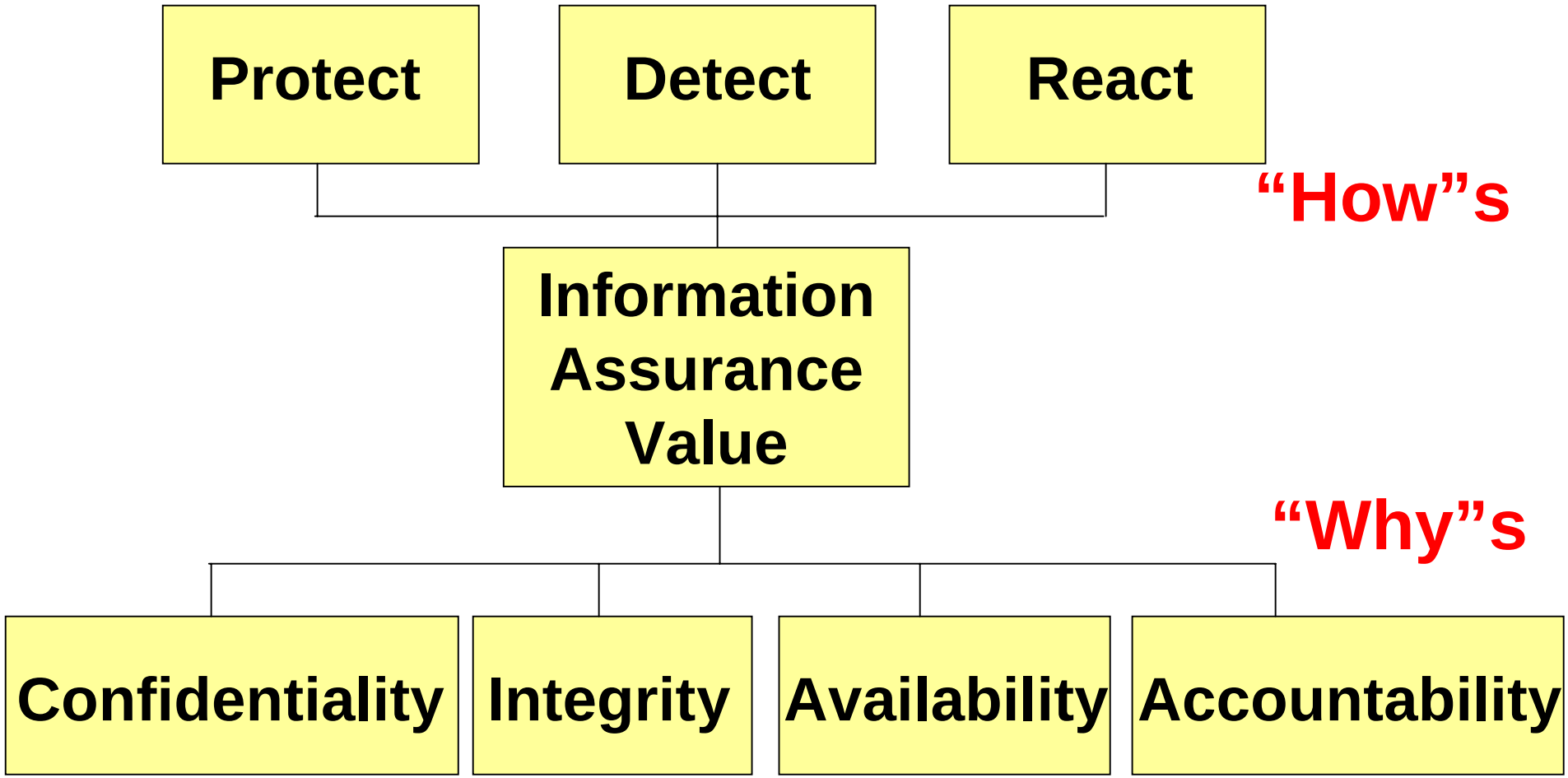
IA Metric Components



Information Assurance Value



“Why”s to “How”s


Protect
Detect
React
“How”s
Information Assurance Value
“Why”s
Confidentiality
Integrity
Availability
Accountability

Streamlined Metrics

1. Review / Inspection of Security Policy
2. Effectiveness against Unauthorized Access or Disclosure
3. Effectiveness against Attack on Data
4. Effectiveness against Attack on System
5. Effort to penetrate to a given level of Access (Privileged, Root, etc.)
6. Effectiveness of Authentication

IA OT&E Test Standards

- Review / Inspection of Security Policy and Procedures
- System Scans
- Penetration Tests
  - Insider
  - Outsider
- Password Cracking
- Detection/Recovery Time

Threat-Risk Assessment Matrix

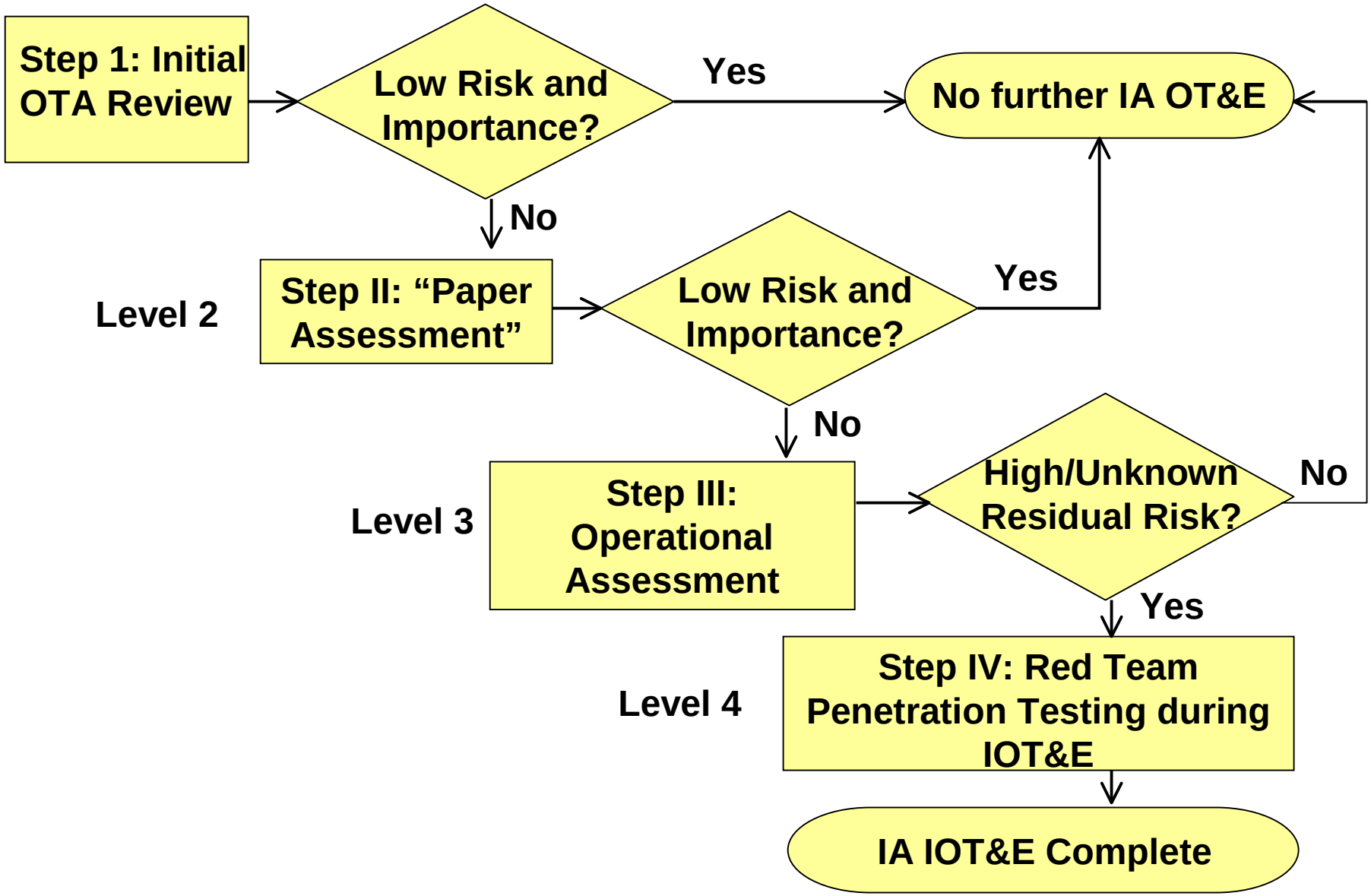
(Higher Level = Higher Risk)

Threat Impact	Likelihood of Threat Penetration		
	Low	Medium	High
Low	Level 1 (None)	Level 2 (Low)	Level 3 (Moderate)
Moderate	Level 2 (Low)	Level 3 (Moderate)	Level 4 (High)
Severe	Level 3 (Moderate)	Level 4 (High)	Level 4 (High)

IA OT&E at the Different Risk Levels

- **Level 1**
  - Exempt from further testing
- **Level 2**
  - Paper Assessment based on system documentation. Similar in scope to DITSCAP Phase 1 vulnerability assessment
- **Level 3**
  - System level assessment similar in scope to DITSCAP Phase 2 vulnerability assessment
- **Level 4**
  - Similar in scope to DITSCAP Phase 3 vulnerability assessment (Level 3 plus Red Team penetration tests)

IA Process with Risk Levels



Remaining Issues

- **How complete are the metrics?**
  - **There will always be the need for flexibility**
- **How often must IA OT&E be repeated?**
- **How can compatibility with DITSCAP be improved?**
- **Which organization(s) will maintain the IA database?**
  - **What will be the format?**
- **Others?**

Back-ups

IA OT&E Metrics

1A. Effectiveness of security policy in preventing unauthorized access: all test standards met?
1B. Effectiveness of system's defense in depth: all test standards met?
2A. Effectiveness of system in preventing unauthorized access (Insider and Outsider): acceptable or not acceptable?
2B. Effectiveness of system in preventing unnecessary disclosure of system information: acceptable or not acceptable?
3A. Ability to detect information degradation/corruption/attack: acceptable or not acceptable?
3B. Time (thresholds set by the user) to respond to information degradation/corruption
3C. Time (threshold set by the user) to restore degraded, corrupted information
4A. Ability to detect system degradation/corruption/attack: acceptable or not acceptable?
4B. Time (threshold set by the user) to respond to system degradation/corruption.
4C. Time (threshold set by the user) to restore critical functionality in a degraded, corrupted system
4D. Time (threshold set by the user) to restore full functionality in a degraded, corrupted system
5. Effort (low, medium, high) to penetrate to a given level of access
6. Effectiveness of authentication?

Example IA Metric with Test Standards

IA OT&E Metric	Test Standard
2A. Effectiveness of system in preventing unauthorized access (from both Insider and Outsider): acceptable or not acceptable?	• System Test - for low risk/low impact systems only • Vulnerability Analysis / Penetration Test - all others (as required; degree TBD; Inside and Outside) • List severity of Known Vulnerabilities; none, low, medium, or high
2B. Effectiveness of system in preventing unnecessary disclosure of information; acceptable or not acceptable?	• System Test - for low risk/low impact systems only • Vulnerability Analysis / Penetration Test - all others (as required; degree TBD)

IA Operational Test Level Process