USMC Information Assurance Operational Testing and Training Strategy

Col. John R. Garvin

Director MCOTEA

and

Mr. Peter H. Christensen

Assistant Scientific Advisor

16 August 2001

MITRE

REPORT DOCUMENTATION PAGE

Form Approved OMB No. 0704-0188

1. REPORT DATE (DD-MM-YYYY)	2. REPORT TYPE	3. DATES COVERED (FROM - TO)
16-08-2001		xx-xx-2001 to xx-xx-2001

4. TITLE AND SUBTITLE
USMC Information Assurance Operational Testing and Training Strategy
Unclassified

5a. CONTRACT NUMBER
5b. GRANT NUMBER
5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)
Garvin, John R. ;
Christensen, Peter H. ;

5d. PROJECT NUMBER
5e. TASK NUMBER
5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME AND ADDRESS
Booz Allen & Hamilton
8283 Greensboro Drive
McLean, VA22102

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME AND ADDRESS
Marine Corps Operational Test & Evaluation Activity
,

10. SPONSOR/MONITOR'S ACRONYM(S)
11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
APUBLIC RELEASE
,

13. SUPPLEMENTARY NOTES

14. ABSTRACT
This brieifing discusses MCOTEA's mission and scope, the USMC's high interest programs, cyber threat and network centric warfare, information assurance and joint interoperability.

15. SUBJECT TERMS
IATAC COLLECTION; information assurance; MCOTEA; cyber threat; network centric warfare; joint interoperability; ia metrics

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE	Public Release	27	Fenster, Lynn lfenster@dtic.mil
Unclassified	Unclassified	Unclassified			19b. TELEPHONE NUMBER International Area Code Area Code Telephone Number 703767-9007 DSN 427-9007

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 074-0188

1. AGENCY USE ONLY (Leave blank)	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	8/16/2001	Briefing 8/16/2001

4. TITLE AND SUBTITLE
USMC Information Assurance Operational Testing and Training Strategy

5. FUNDING NUMBERS

6. AUTHOR(S)
Garvin, Col. John R.; Christensen, Peter H.

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

Booz Allen & Hamilton
8283 Greensboro Drive
McLean, VA 22102

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)

Marine Corps Operational Test & Evaluation Activity

10. SPONSORING / MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES

12a. DISTRIBUTION / AVAILABILITY STATEMENT
Approved for public release; Distribution unlimited

12b. DISTRIBUTION CODE
A

13. ABSTRACT *(Maximum 200 Words)*

This brieifing discusses MCOTEA's mission and scope, the USMC's high interest programs, cyber threat and network centric warfare, information assurance and joint interoperability.

14. SUBJECT TERMS
IATAC Collection, information assurance, MCOTEA, cyber threat, network centric warfare, joint interoperability, ia metrics

15. NUMBER OF PAGES
26

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
UNCLASSIFIED	UNCLASSIFIED	UNCLASSIFIED	UNLIMITED

Outline

- MCOTEA: The Mission and Scope
- USMC High Interest Programs
- OTA Partners
- The “Cyber” Threat and Network Centric Warfare
- The Emerging Challenge: Information Assurance
- Leveraging the DOD Process
- DOT&E IA OT Policy
- DOT&E IA Metrics Guidelines
- DITSCAP Process
- Joint Interoperability
- Leveraging and Integrating into the MCOTEA Process
- Conclusions

Mission

- "To support the material acquisition process established by MCO P5000.22 by managing the Marine Corps Operational Test (OT) Program for Acquisition Categories (ACAT) I through ACAT IV, less the OT of manned aircraft, and to perform such other functions as directed by the CMC."

Workforce

- 20 of 27 Marines, 11 of 24 Civil Service, 9 Contractors

Scope

- At least *125* programs in varying stages of test
- Great majority non-oversight ACAT III/IV programs

I

AAAV

ACAT ID $4 B

LPD17

ACAT ID $B

II

MTVR

ACAT II $1.4 B

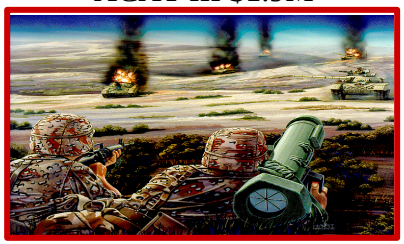
MPF(E)

ACAT III $50M

III

Predator

ACAT III $1.9M



MLS

ACAT IV $6 M

BOOT

ACAT IV $2 M

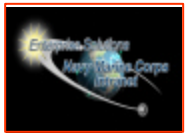
JSCS

ACAT IV $10 K

IV

Across all ACATs

High Interest Programs

-  Advanced Amphibious Assault Vehicle (AAAV)
-  Lightweight 155 Howitzer (LW-155)
-  Internally Transportable Vehicle (ITV)
-  Maritime Prepositioning Force, Enhanced, (MPF(E))
  USNS GySgt Fred W. Stockham
-  Navy, Marine Corps Intranet (NMCI)
-  LPD-17 Amphibious Transport Dock

OTA PARTNERS

ATEC

MGEN J. MARCELLO

Auth: 1385

DOT&E

The Honorable

MR. T. CHRISTIE

OPTEVFOR

RADM R. BESAL

Auth: 345

MCOTEA

COL J. GARVIN

Auth: 50

JITC

COL B. OSLER

Auth: est 250

AFOTEC

MGEN W. PECK

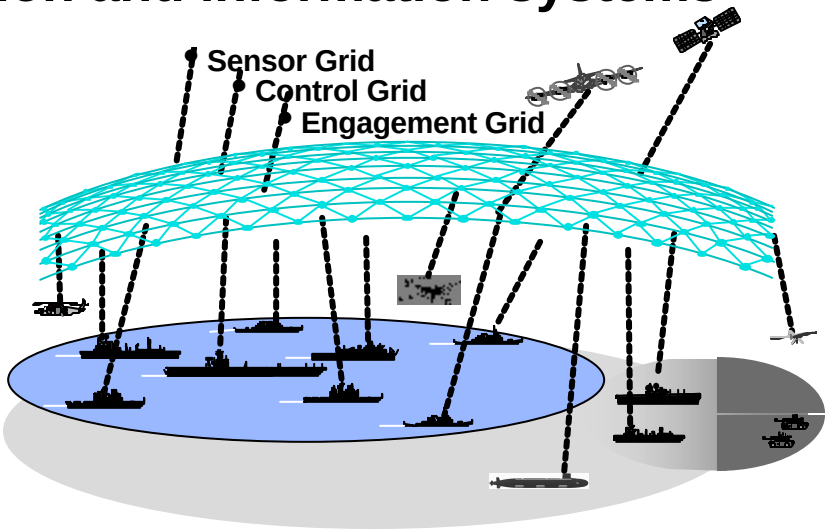
Auth: 901

What is the Commercial IW Threat?

- 40% Internal, 40% Dial UP and 20% Internet
  - Hackers, Crackers, Hacktivist, Terrorist and Corporate Espionage
- "Russian Mafia" `Interactive Week, July 16, 2001`
  - Operates in 50 Countries: Infiltrate businesses and launch internet attacks
    - Ministry of Internal Affairs estimates that 5,600 criminal groups (more than 100,000 individuals) are involved in money laundering, drugs, and extortion
  - Eastern Europeans Crackers among the most skillful in the world
    - Led by former KGB Agents: Some even plant employees inside targeted companies
  - Few cases are prosecuted and thus few deterrents to foreign hackers!

Network Centric Warfare relies on Effective Information Operations

- Joint Vision 2010: Focus is Network Centric Warfare (NCW)
  - Distributed sensors and shooters with precision weapons
- Dependent upon effective Information Operations (IO)
  - Actions taken to affect adversary information and information systems while defending ones own information and information systems



MITRE

The Emerging Challenge: Information Assurance

- Effective conduct of IO for NCW requires that combat forces be reliably "connected" to the supporting infrastructure
- Information Assurance is a subset of IO:
  - IO that protect and defend information and information systems (IS) by ensuring their ***availability, integrity, confidentiality, authentication, non-repudiation***. This includes providing for the restoration of IS by incorporating ***protection, detection and reaction capabilities***
- NCW relies on distributed platforms and sensors to detect, locate, target and eliminate enemy with precision munitions
  - Infiltrating the network could allow the enemy to exploit your sensors and understand your force disposition
  - Simply disrupting the network isolates sensors from weapon systems and renders your force impotent !

". . . attaining one hundred victories in one hundred battles is not the pinnacle of excellence. Subjugating the enemy's army without fighting is the true pinnacle of excellence."
Sun Tzu, The Art of War

MITRE

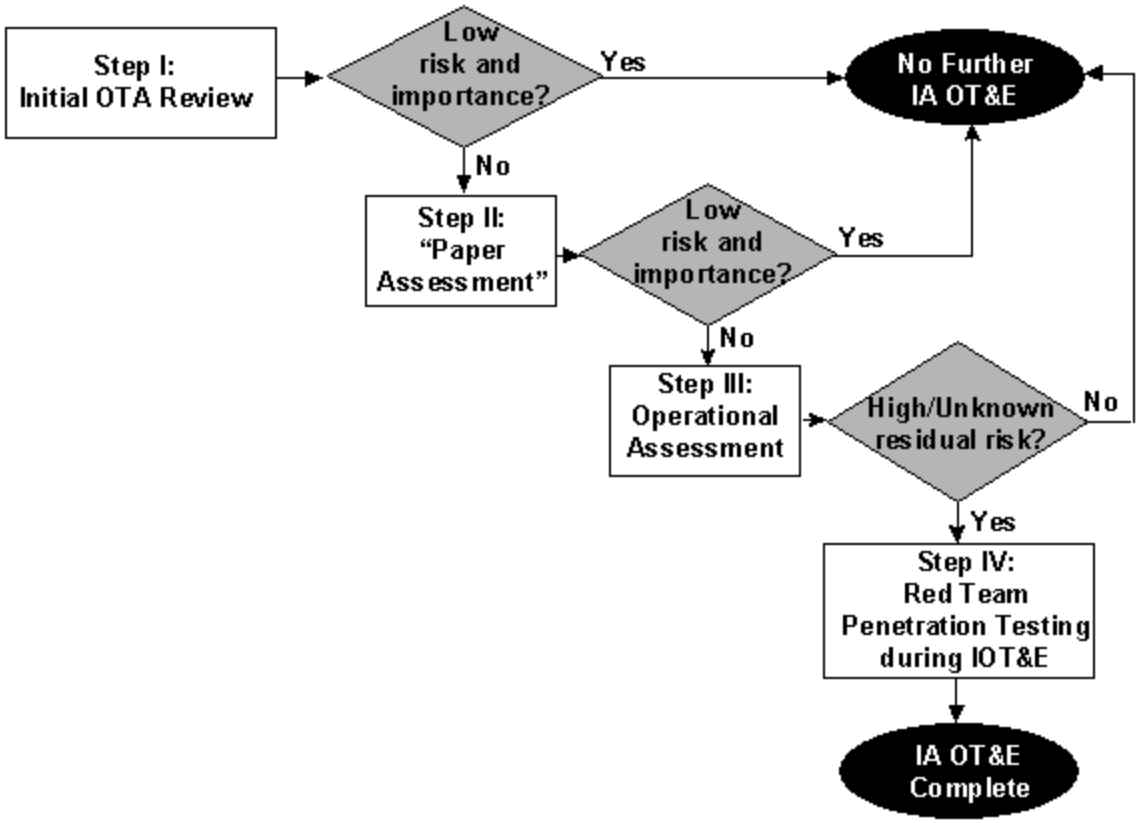
MCOTEA Approach: Leverage the Acquisition Process for IA

- Effective implementation of NCW requires we consider Security, Interoperability and Information Assurance collectively as we work to acquire systems
- Key documents drive the acquisition and testing process:
  - DITSCAP DOD 8510.1
  - CJCSI 6212.01B Interoperability and Supportability of NNSS and IT Systems (08 May 2000)
  - DOD CIO GIG IA Policy Memo. No. 6-8510 (16 June 2000)
  - DOT&E Policy for OT&E of IA (17 Nov 1999)
  - DOT&E Guidelines on Metrics for OT of IA (19 Jan 2001)
- MCOTEA must integrate DOD and JCS mandates into a cohesive OT&E Strategy and
  - Coordinate strategy with acquisition and testing stakeholders and train the USMC OT&E test force

DOT&E IA OT Policy

- Policy for Operational Test and Evaluation of Information Assurance (17 Nov 1999)
  - Provides Background, Applicability and Scope, Definitions and Implementation
- Applicability
  - ACAT 1 Programs and programs with DOT&E oversight that have yet to reach MS “C”
- Policy describes four implementation steps
  - Step I: Requirements, Threat and Test Documentation Review
  - Step II: Test Strategy Development
  - Step III: Review IA DT&E and Computer Security Certification Results Prior to Entry into OT&E
  - Step IV: Evaluation of IA Vulnerabilities during IOT&E

IA OT Four Step Process



MITRE

DOT&E IA Metrics Guidelines

- Guidelines on Metrics for Operational Testing of Information Assurance (19 Jan 2001)
  - Developed to complement IA Policy
  - Designed to aid testers and evaluators who are not knowledgeable in IA
  - Not all metrics must be measured for every acquisition program
- T&E Community has identified eight potential IA metrics
  - Test Standards are included
- Risk Assessment identifies required metrics!
  - Level 1: No metrics required
  - Level 2: Limited metrics
  - Level 3: Moderate metrics
  - Level 4: All Metrics

DOT&E IA Metrics Guidelines

IA OT Metrics	Description
Metric 1A	Effectiveness of security policy in preventing unauthorized access: all test standards met?
Metric 1B	Effectiveness of system defense in depth: all test standards met?
Metric 2A	Effectiveness of system in preventing unauthorized access (from both insider and outsider) acceptable or unacceptable?
Metric 2B	Effectiveness of system in preventing unnecessary disclosure of system information: acceptable or
Metric 3A	Ability to detect information degradation/corruption/attack: acceptable or unacceptable?
Metric 3B	Time (Thresholds set by the user) to respond to information degradation/corruption.
Metric 3C	Time (Thresholds set by the user) to restore degraded/corrupted information.
Metric 4A	Ability to detect system degradation/corruption/attack: acceptable or not acceptable?
Metric 4B	Time (Thresholds set by the user) to respond to system degradation/corruption.
Metric 4C	Time (Thresholds set by the user) to restore critical functionality into a degraded/corrupted system.
Metric 4D	Time (Thresholds set by the user) to restore full functionality into a degraded/corrupted system.
Metric 5	Effort (low, medium, high) to penetrate to a given level of access.
Metric 6	Effectiveness of authentication?

Metrics by Risk Level
Level 2: Low Risk: Red
Level 3: Medium Risk: Red + Yellow
Level 4: High Risk: All Metrics

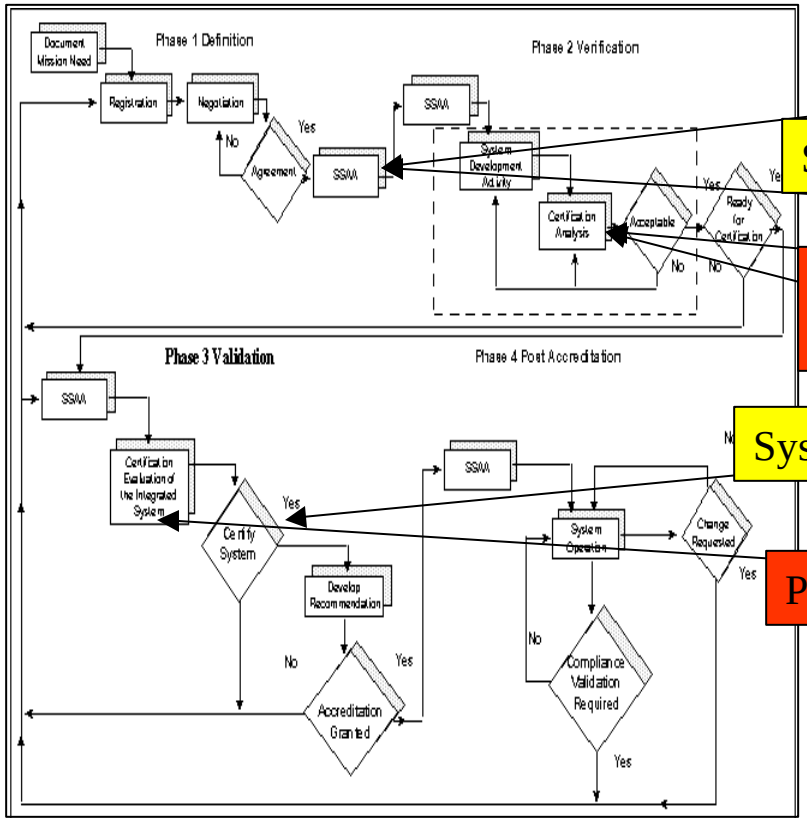
Note: These metrics are more fully developed for inclusion in MCOTEA IA OT SOP.

MITRE

DITSCAP Process

- DoD Information Technology Security Certification and Accreditation Process (DITSCAP) DoD 8510.1
  - All IS, to include stand-alone personal computers, connected systems, and networks, must be accredited
  - The standard DoD Approach for identifying information security requirements, providing security solutions, and managing information technology system security
- USMC Project Officer's Certification and Accreditation Handbook (Sep 2000)
- Four Phase Process
  - Phase 1: Definition
  - Phase 2: Verification
  - Phase 3: Validation
  - Phase 4: Post Accreditation
- Changes may warrant beginning a new DITSCAP cycle

Leveraging DITSCAP for IA

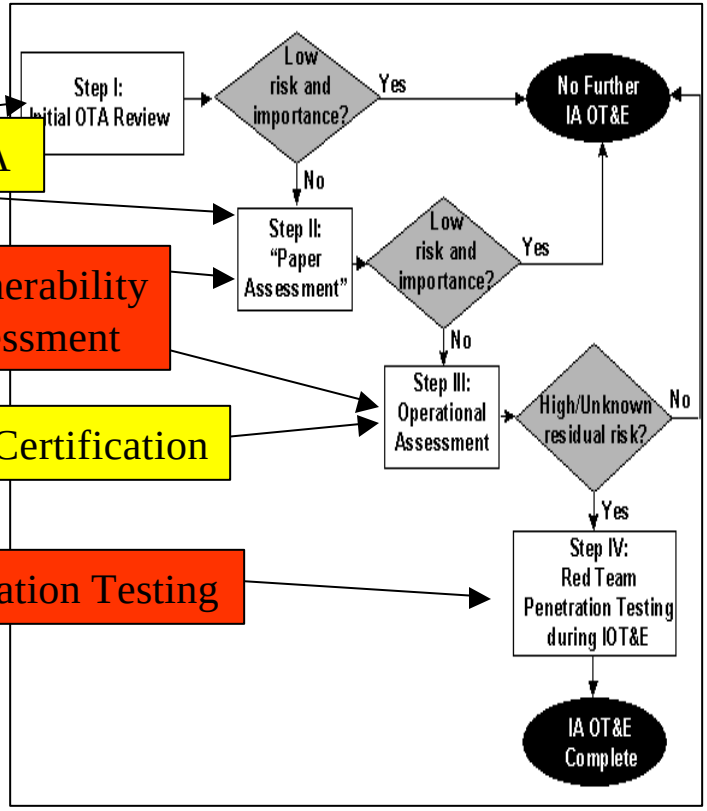


SSAA

Vulnerability Assessment

System Certification

Penetration Testing

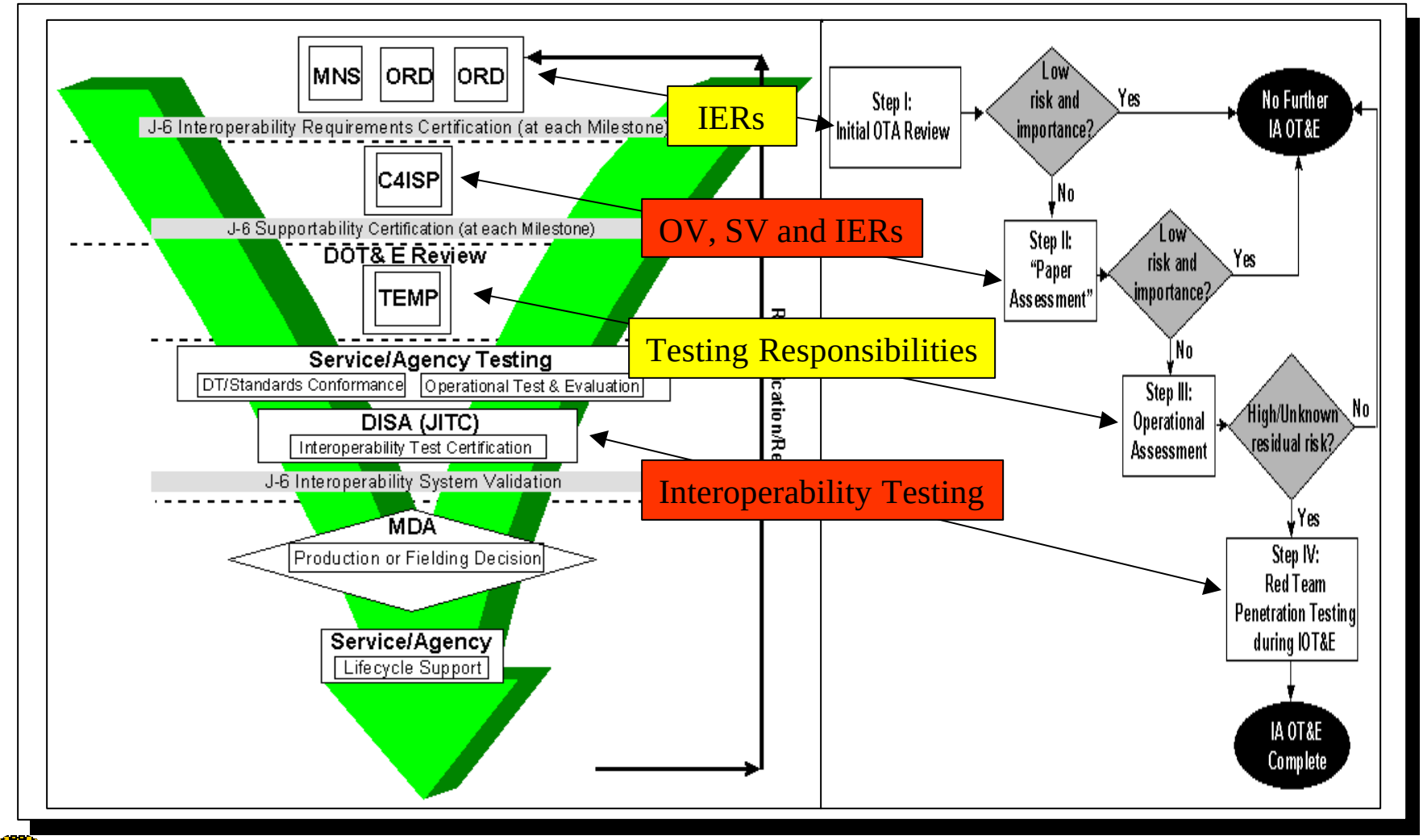


MITRE

Joint Interoperability

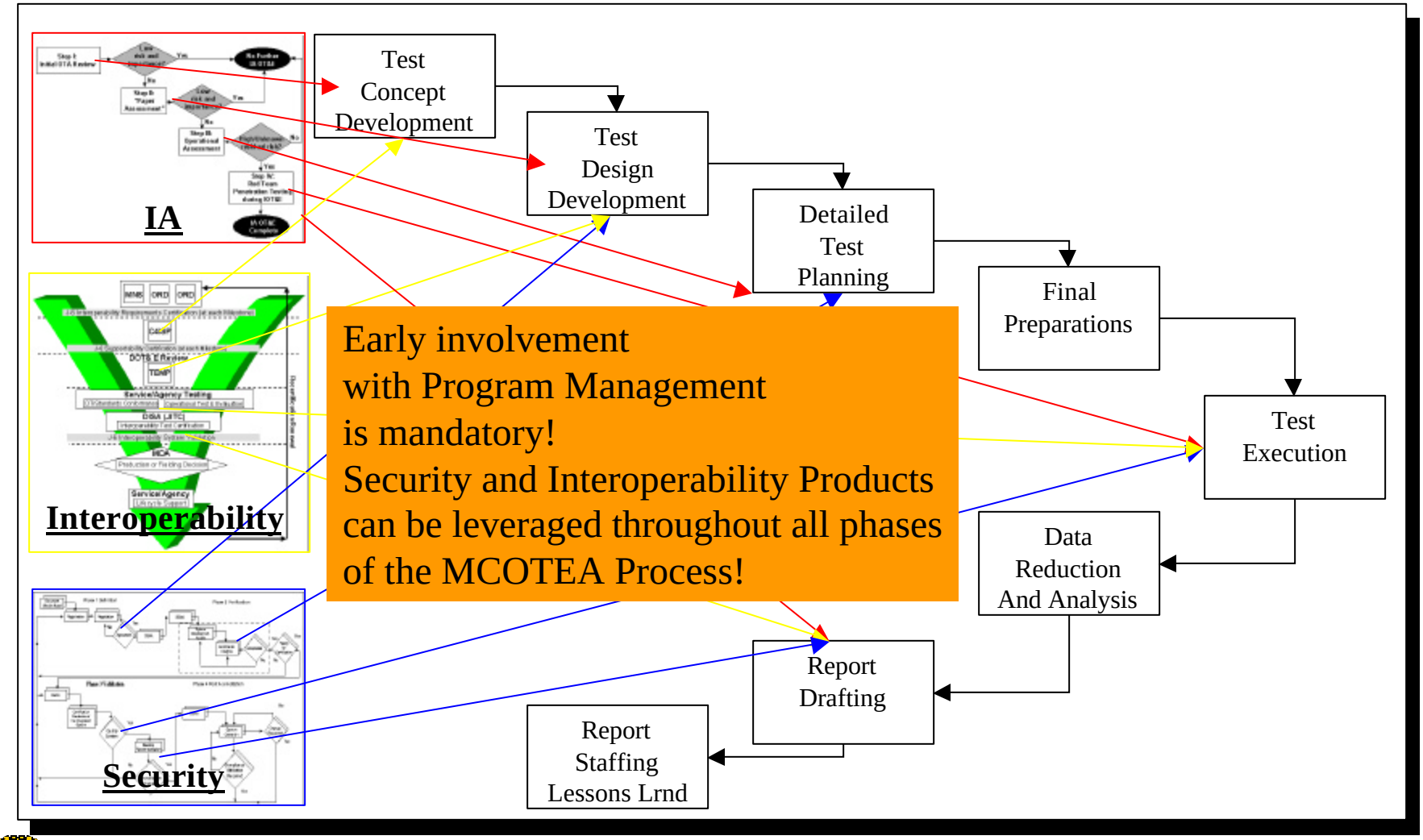
- CJCSI 6212.01B Interoperability and Supportability of National Security Systems and Information Technology Systems (08 May 2000)
  - Establishes policies and procedures for J-6
    - Interoperability requirements certification of MNS, CRD and ORDs
    - Supportability certification of C4ISPs
    - Interoperability system validation
  - Details a methodology to develop interoperability KPPs derived from a set of top-level IERs based on the format and content of the C4ISR integrated architecture products

Leveraging the J-6 Certification and Validation Process



MITRE

Integrating Security, Interoperability and IA into the MCOTEA Process



MITRE

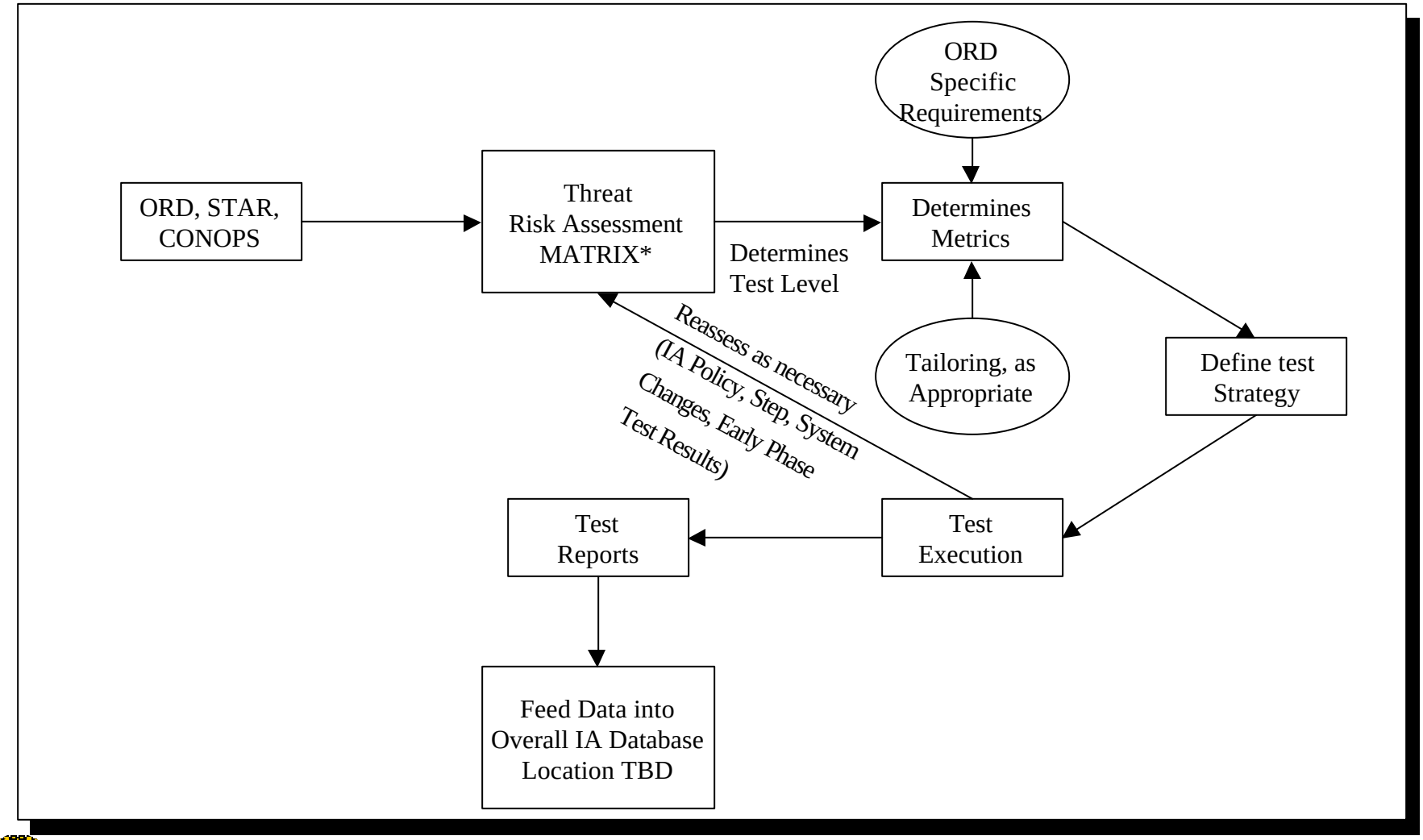
Conclusions

- There are lots of moving parts!
- MCOTEA strategy is intended to be tailorable and non threatening
  - Provides MCOTEA an opportunity to report to the MDA regarding how well policies are being implemented
    - Failure to implement these policies puts the war fighter at risk and could adversely impact USMC operations in a Joint Environment
- Early involvement with DITSCAP and Joint Interoperability is the key
  - Allows MCOTEA to leverage other activities and makes best use of limited resources
  - Education and training is critical!
  - MCOTEA is coordinating with JITC, COTF, AFOTEC, ATEC, MCCDC and MCSC to refine this strategy!

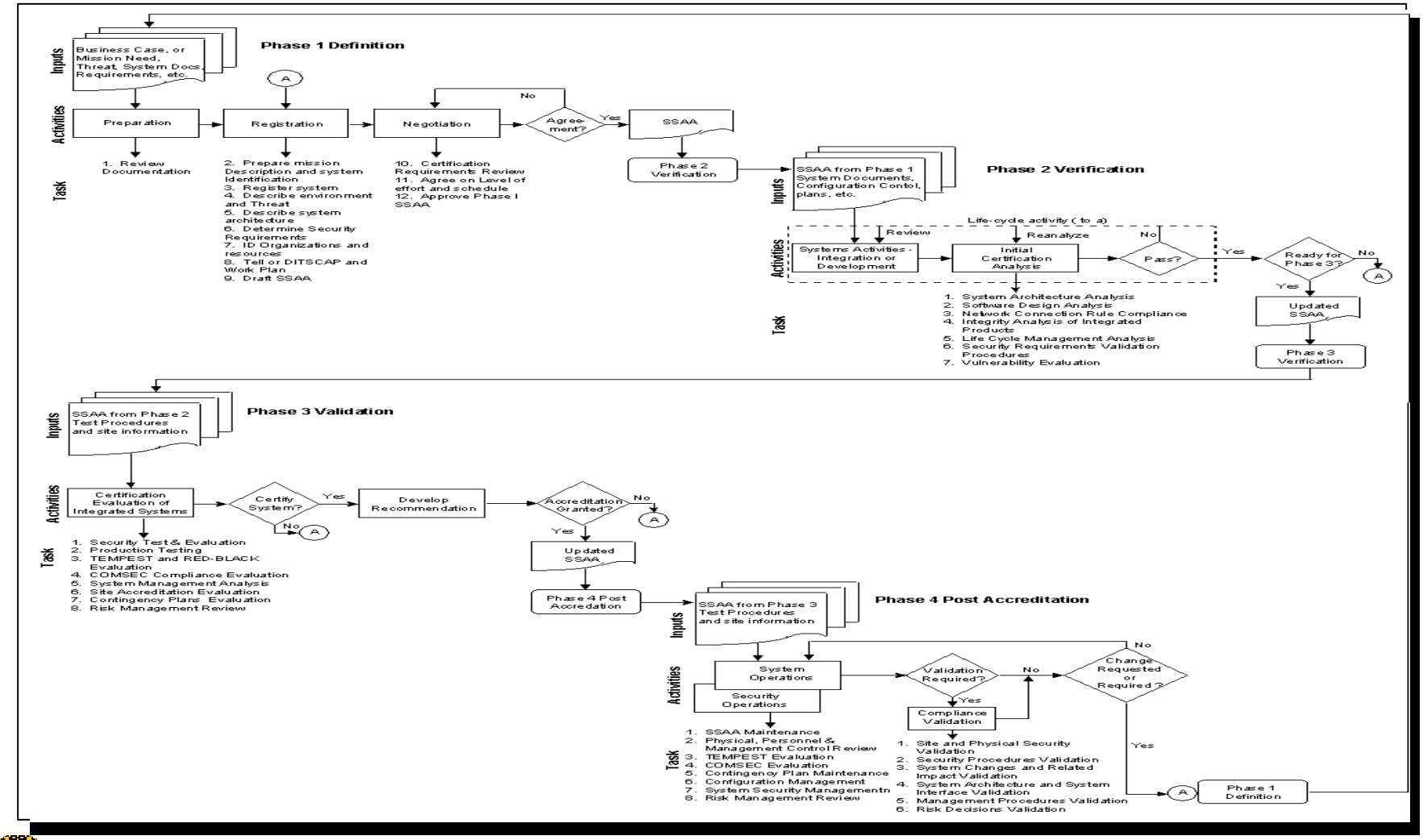
Backups

MITRE

IA Metrics Process

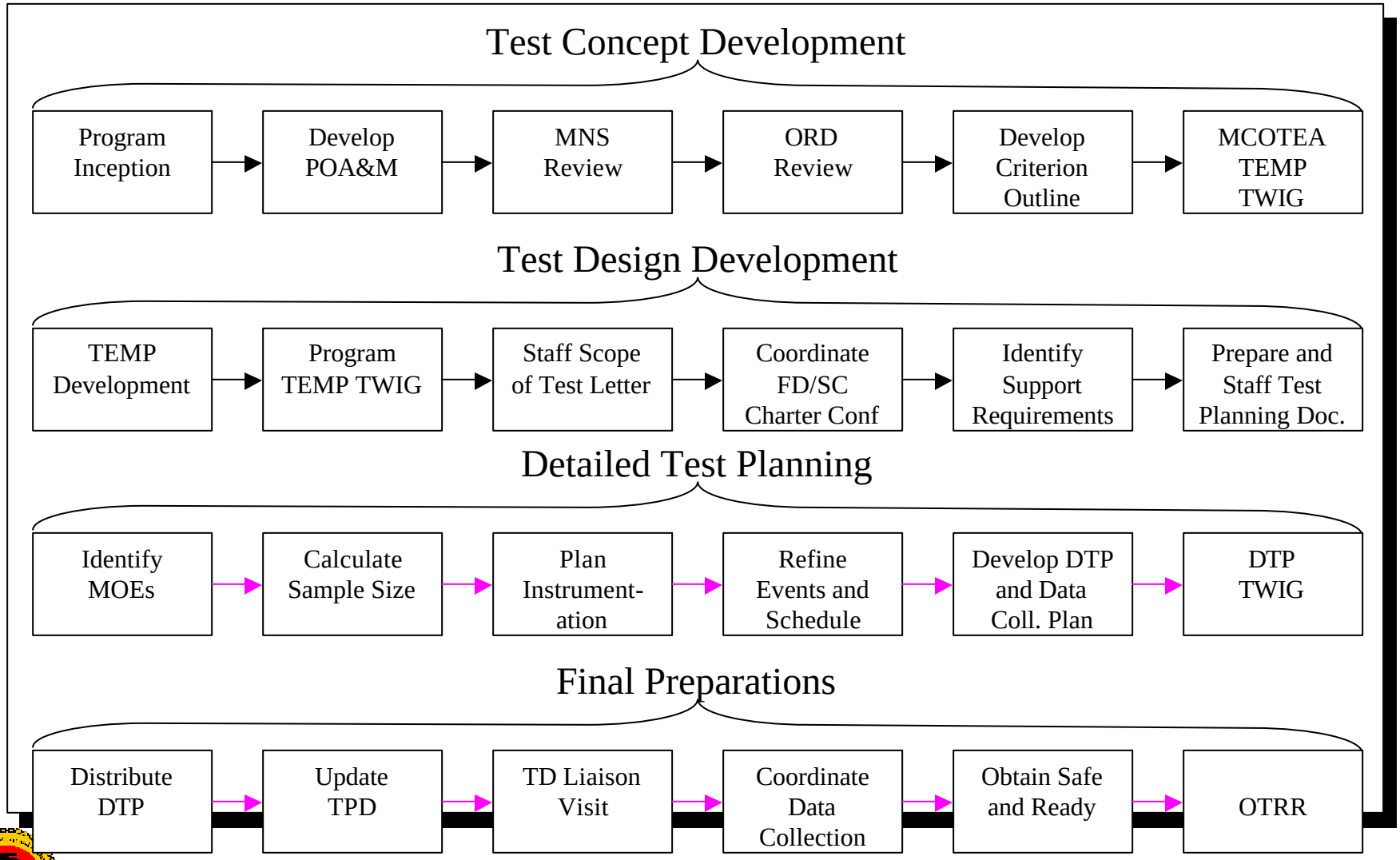


DITSCAP Four Phase Process



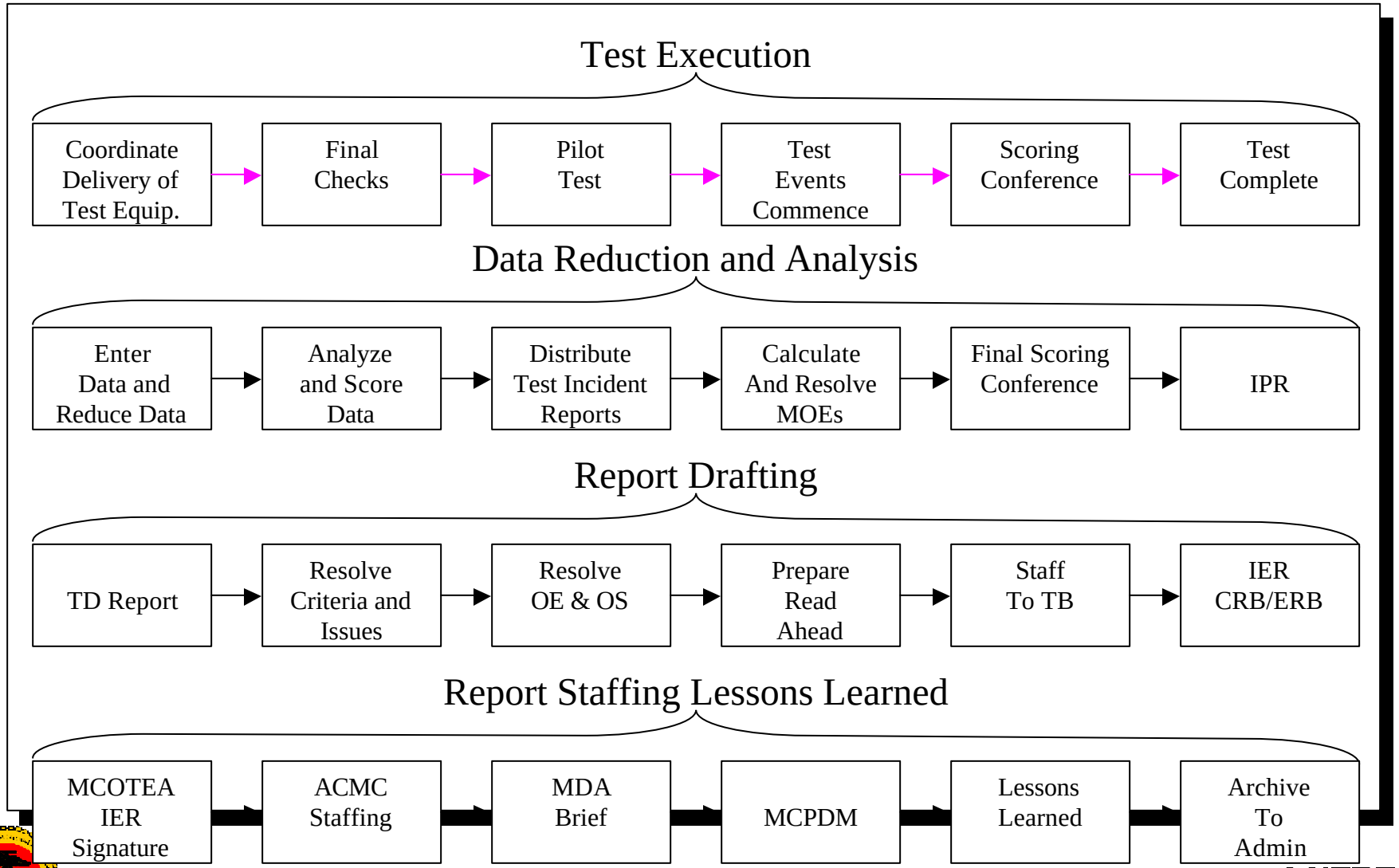
MITRE

Simplified MCOTEA Process



MITRE

Simplified MCOTEA Process (Concluded)



What are Commercial Organizations doing?

- Corporations are increasing computer security budgets.
  - Recent Gartner reports computer security expenditures will average 4 percent of annual revenue by 2011
    - A tenfold increase from today
- It is not sufficient just to identify and seal security holes
  - A system administrator or security officer must stand watch for "leaks" or intrusions
- Security intelligence professional services are being created
  - Assume operational responsibility for securing a customer's Web site or network
  - Internet Security intelligence services are modeled after military intelligence-gathering apparatus
  - A good security intelligence service offers alerts and recommends how to address security incidents