

N92-12030

AISS TECHNOLOGY ROLE

CONTROL CENTER TECHNOLOGY

MOD CONTROL CENTER AUTOMATED INFORMATION SYSTEMS SECURITY EVOLUTION

RICH OWEN
MOD COMPUTER SECURITY OFFICIAL

520-14
39622
P-25
N2185000

PURPOSE

- **HIGHLIGHT THE ROLE OF THE TECHNOLOGY INFUSION PROCESS IN FUTURE CONTROL CENTER AUTOMATED INFORMATION SYSTEMS (AIS)**

OVERVIEW

- GOALS
- BACKGROUND
- THREAT
- MOD'S AISS PROGRAM
- TQM
- SDLC INTEGRATION
- PAYBACK
- FUTURE CHALLENGES
- BOTTOM LINE

GOALS

- **IMPROVE THE CONFIDENTIALITY, INTEGRITY, & AVAILABILITY OF AIS THROUGH TECHNOLOGY**
- **EVOLVE AISS TECHNOLOGY THROUGH THE RISK MANAGEMENT PROCESS**

BACKGROUND

PAST

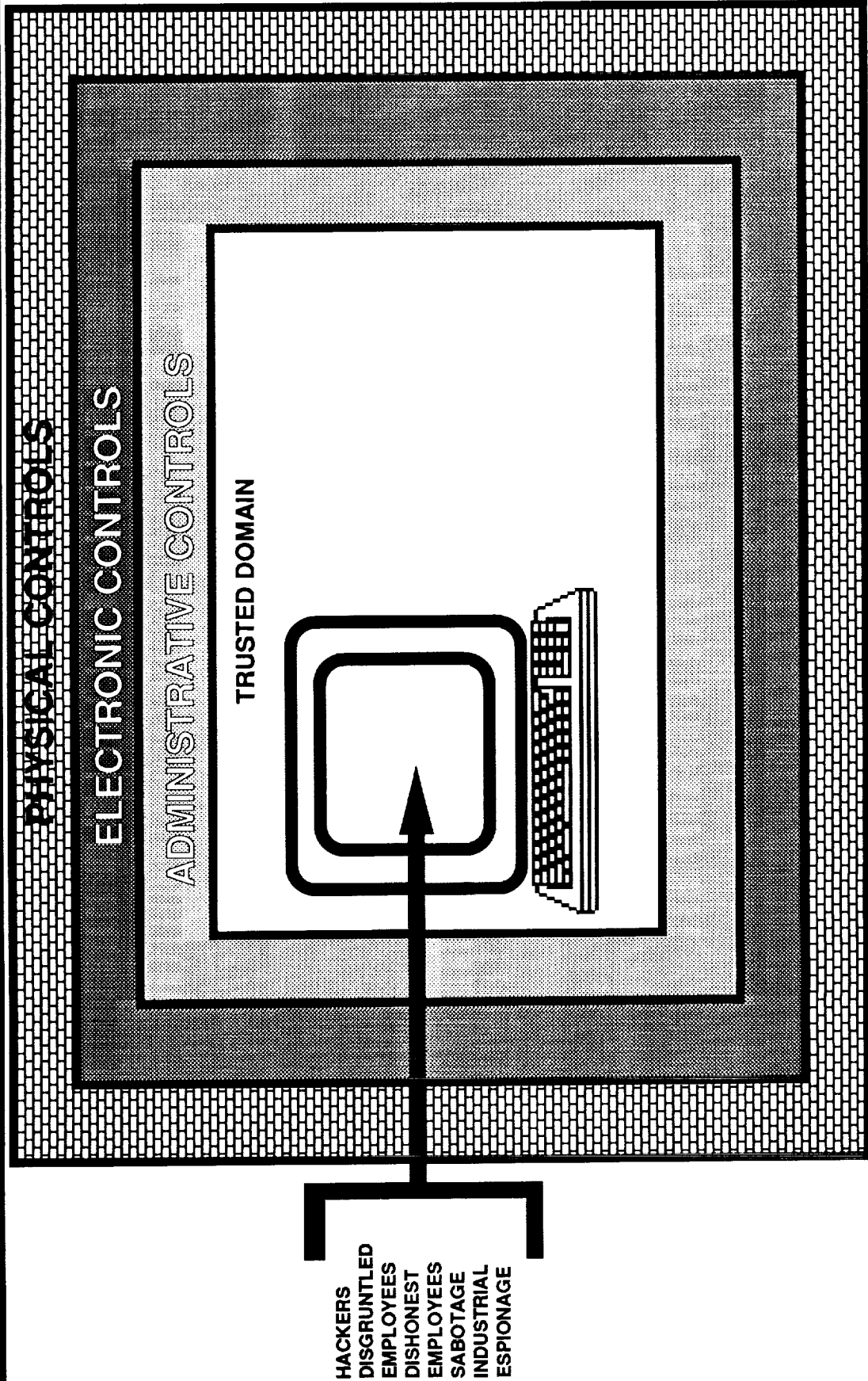
- OUR DOD HERITAGE
 - PROCEDURAL
 - EMPHASIS ON ACCESS CONTROL
 - MANDATORY COMPLIANCE

BACKGROUND

PRESENT

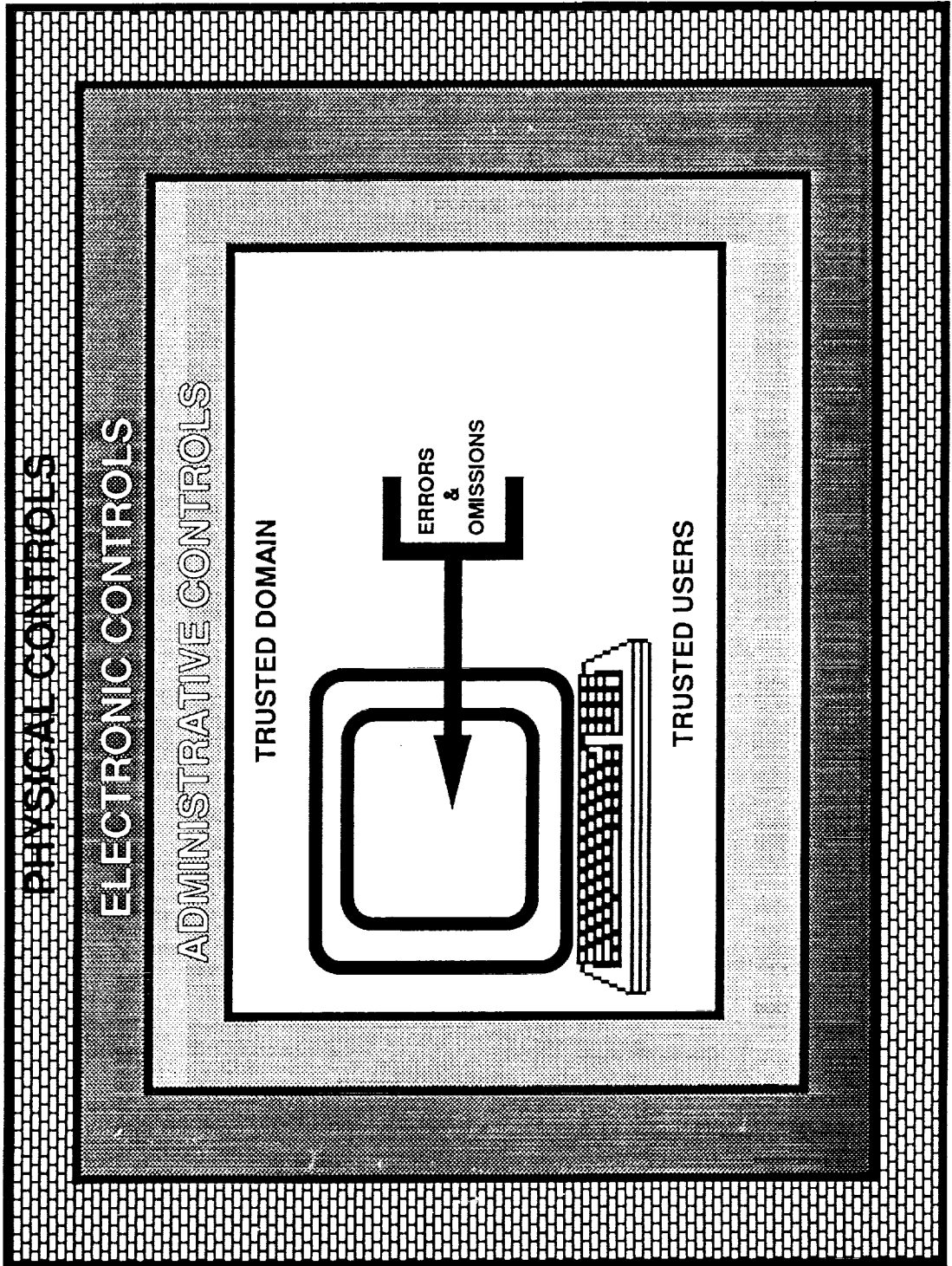
- MANDATE FOR CONFIDENTIALITY, INTEGRITY, & AVAILABILITY
- COMPUTERS AT RISK
- A NEW PHILOSOPHY
 - NO LONGER COMPLIANCE BASED
 - EMPHASIS ON RISK MANAGEMENT

EXTERNAL THREAT



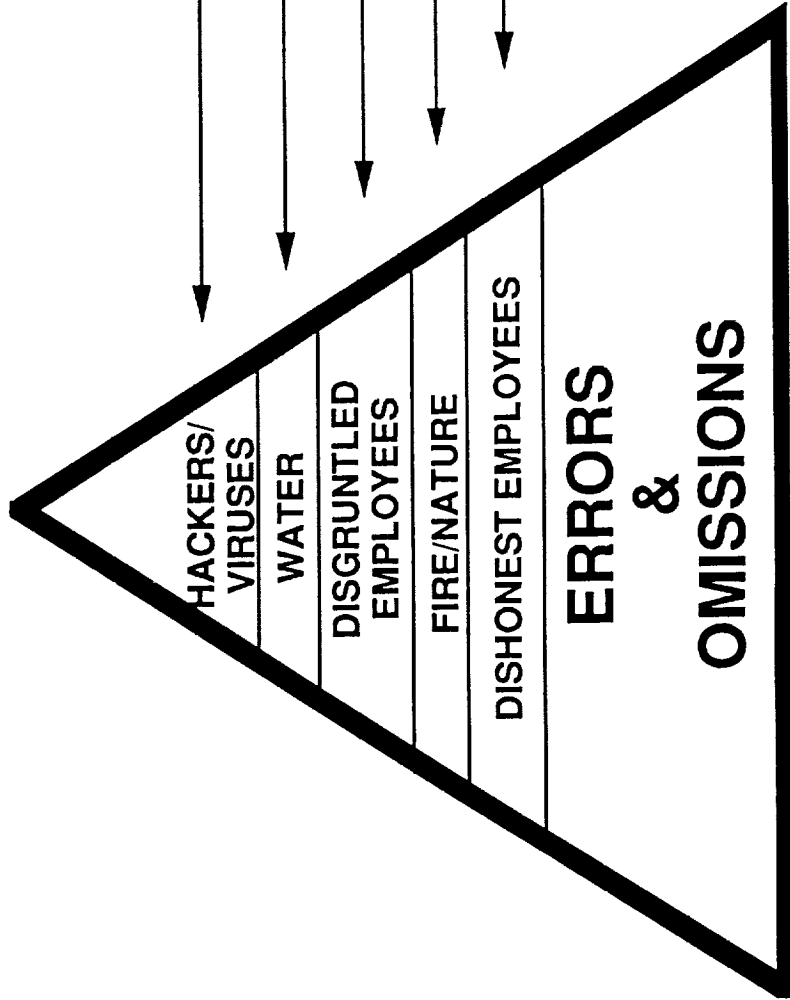
- HACKERS
- DISGRUNTLED EMPLOYEES
- DISHONEST EMPLOYEES
- SABOTAGE
- INDUSTRIAL ESPIONAGE

INTERNAL THREAT



THREAT ANALYSIS

THE CHANGING ENVIRONMENT



INCIDENTS

| | 87 | 88 | 89 | 90 | 91 |
|-------------------------------|----|----|----|----|----|
| HACKERS/VIRUSES | | 2 | 2 | 12 | 24 |
| WATER | 1 | | | | |
| DISGRUNTLED EMPLOYEES | | .5 | | | |
| FIRE/NATURE | | | | | |
| DISHONEST EMPLOYEES | | .5 | | | |
| ERRORS & OMISSIONS | | | | | |
| UNKNOWN TOTAL | | | | | |

POLICY

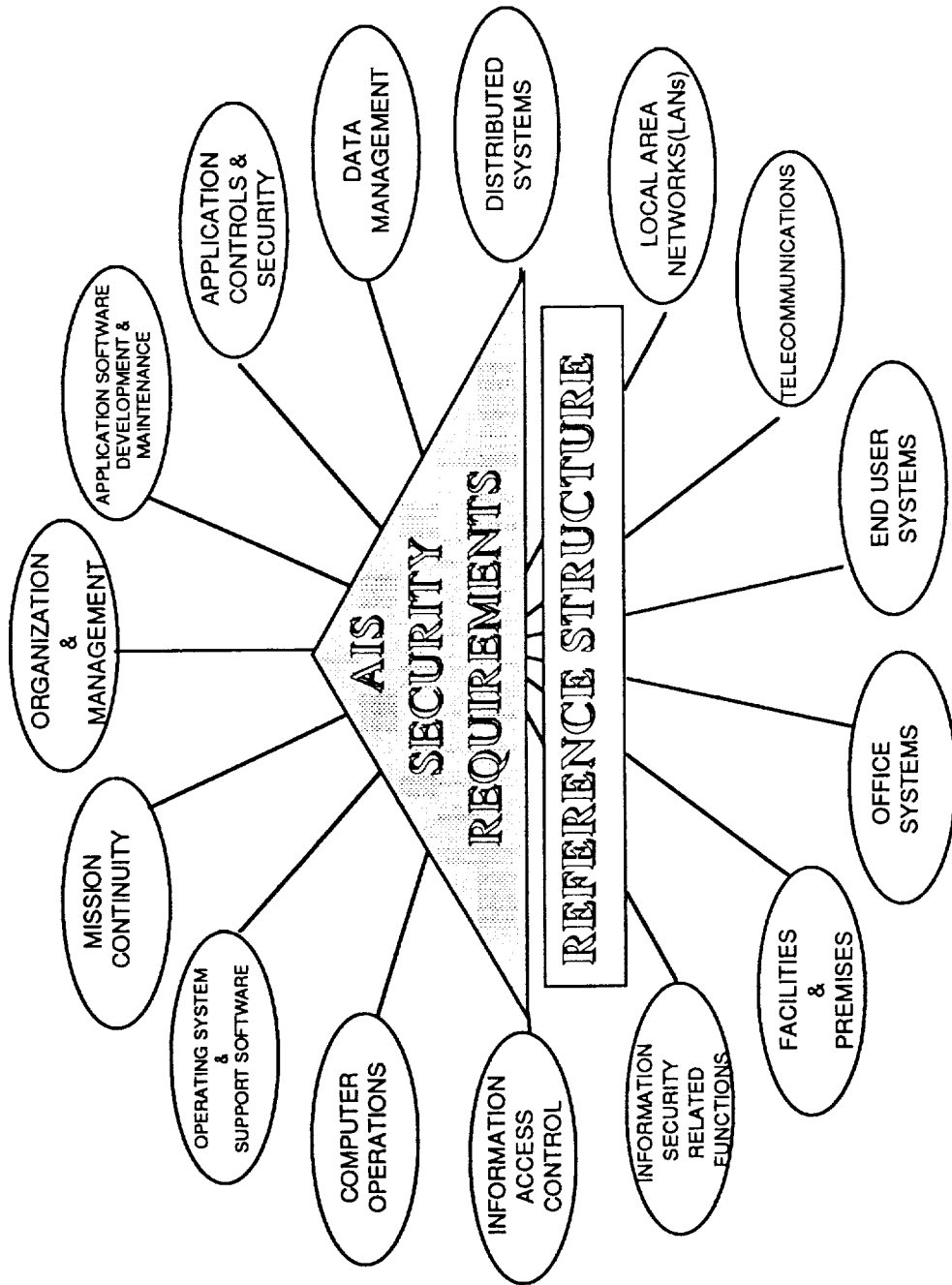
- MOD LEADERSHIP STATEMENT
24 OCT 90:

"We want technical, not procedural solutions for AIS security!"

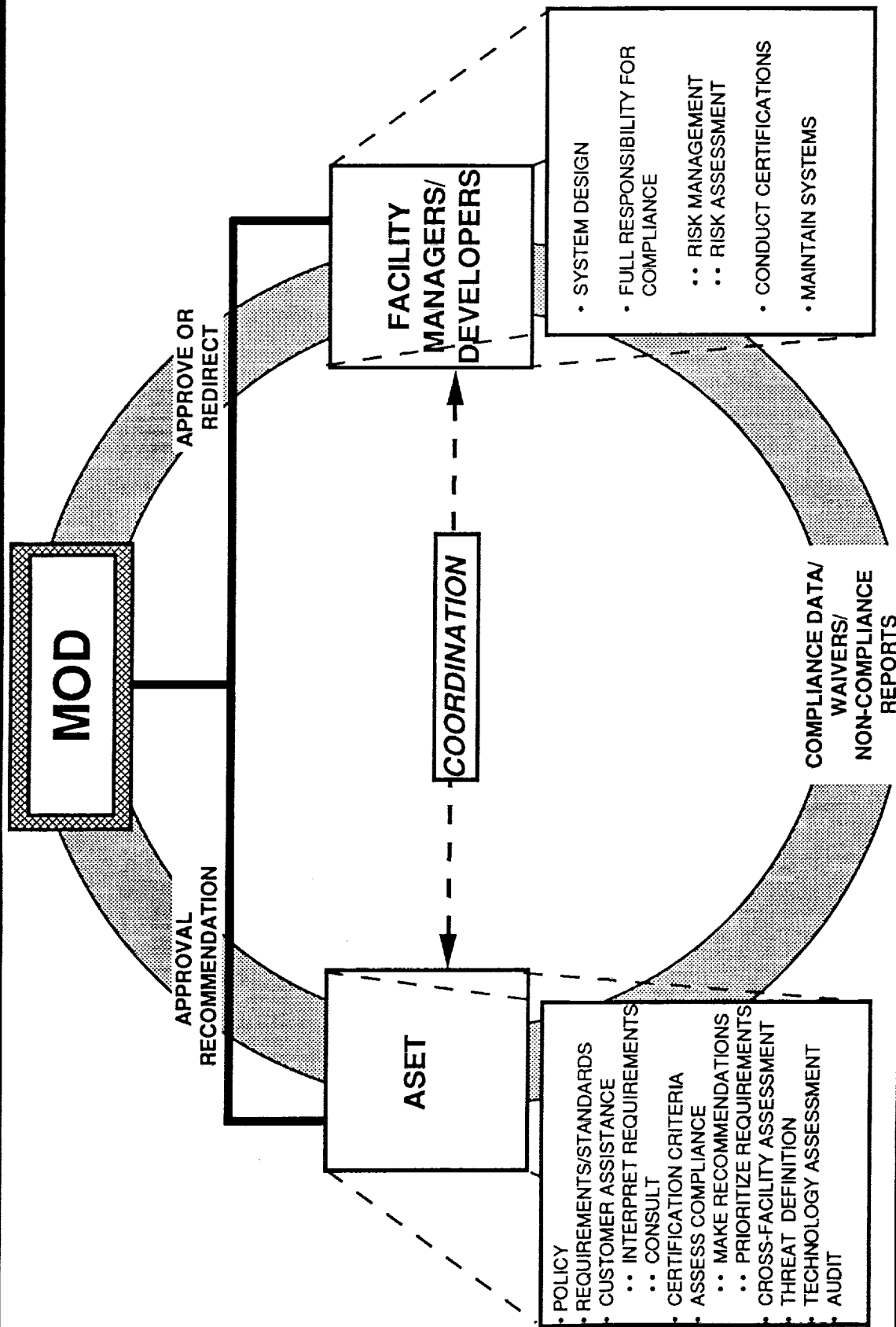
POLICY

- PINK BOOK
 - ADMINISTRATIVE, ELECTRONIC, & PHYSICAL
 - DAY-TO-DAY OPERATIONS
- REFERENCE STRUCTURE
- SPIN-OFF CALLS FOR AISS TECHNOLOGY

REFERENCE STRUCTURE



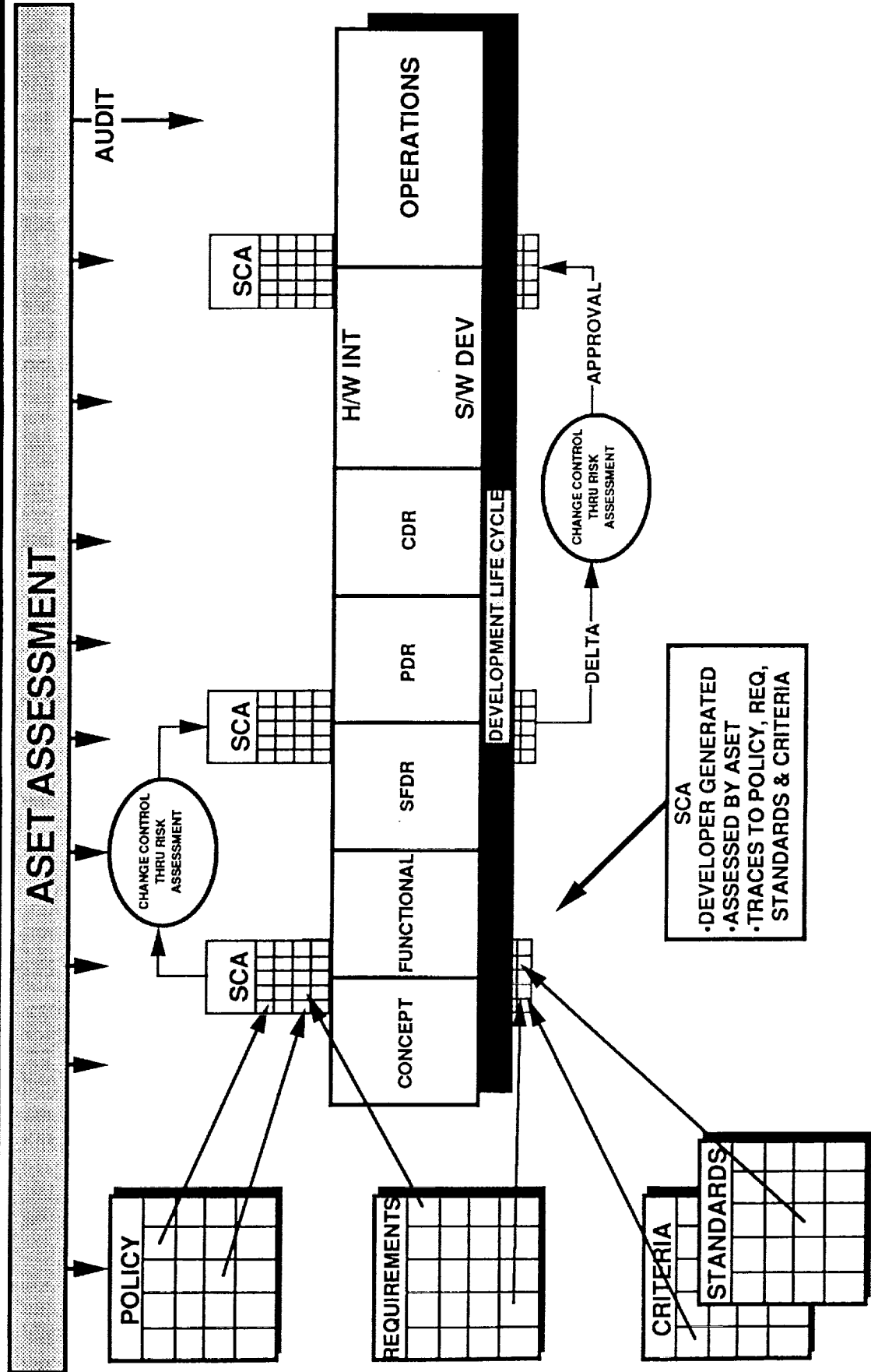
INSTITUTIONALIZATION



TQM

- **ORIENTATION TO THE ULTIMATE CUSTOMER**
- **IN CONJUNCTION WITH THE FACILITY MANAGEMENT**

SDLC AISS INTEGRATION



REAL WORLD

- **RETROFIT FOR COMPLIANCE IS COST PROHIBITIVE**
- **WORKABLE TRANSITION FROM COMPLIANCE TO RISK MANAGEMENT**

CATCH UP

- **IN DEVELOPMENT**
 - **DESIGNED**
 - **FIXED SCHEDULED**
 - **APPORTIONED BUDGET**
- **IN OPERATION**
 - **MUST NOT IMPACT FLIGHT OPERATIONS**
 - **MUST REDUCE RISK**

TECHNICAL SOLUTIONS

EXTERNAL THREAT COUNTERMEASURES

- **USER/HOST AUTHENTICATION:
SMART CARDS**
- **ELECTRONIC TRANSFER
VERIFICATION: DIGITAL
SIGNATURES/ENVELOPES**
- **SYSTEM REDUNDANCY**
- **NON-REPUDIATION**

TECHNICAL SOLUTIONS

INTERNAL THREAT COUNTERMEASURES

- HIGH-LEVEL PROGRAMMING LANGUAGES
- SEI METHODS & PROCEDURES
- DATA INTEGRITY TECHNOLOGY

CONTINUED EVOLUTION

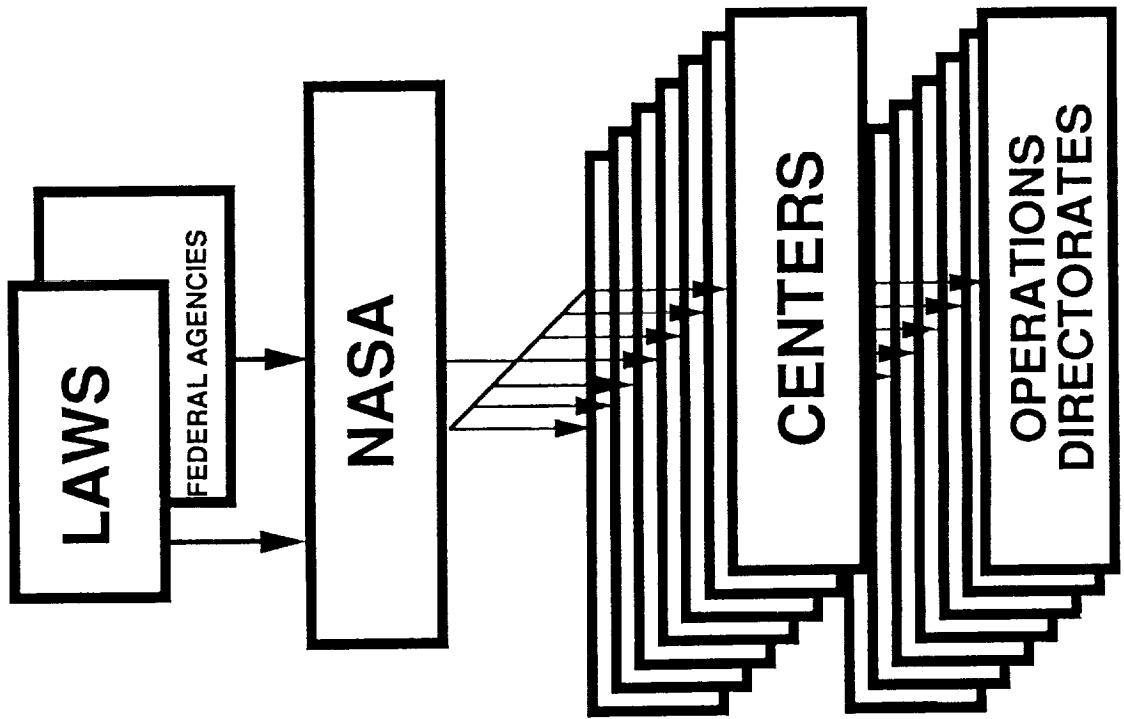
- ANNUAL TECHNOLOGY CONFERENCE
- TECHNOLOGY PROTOTYPING
- TECHNOLOGY ASSESSMENT
- TECHNOLOGY AUDIT

PAYBACK

- RISK MANAGEMENT
- COST EFFECTIVE
- FIX BIGGEST PROBLEMS
- ALLOWS ACTIVE MANAGEMENT PARTICIPATION IN RISK REDUCTION
- PROVIDES MANAGEMENT AN UNDERSTANDING OF VULNERABILITIES

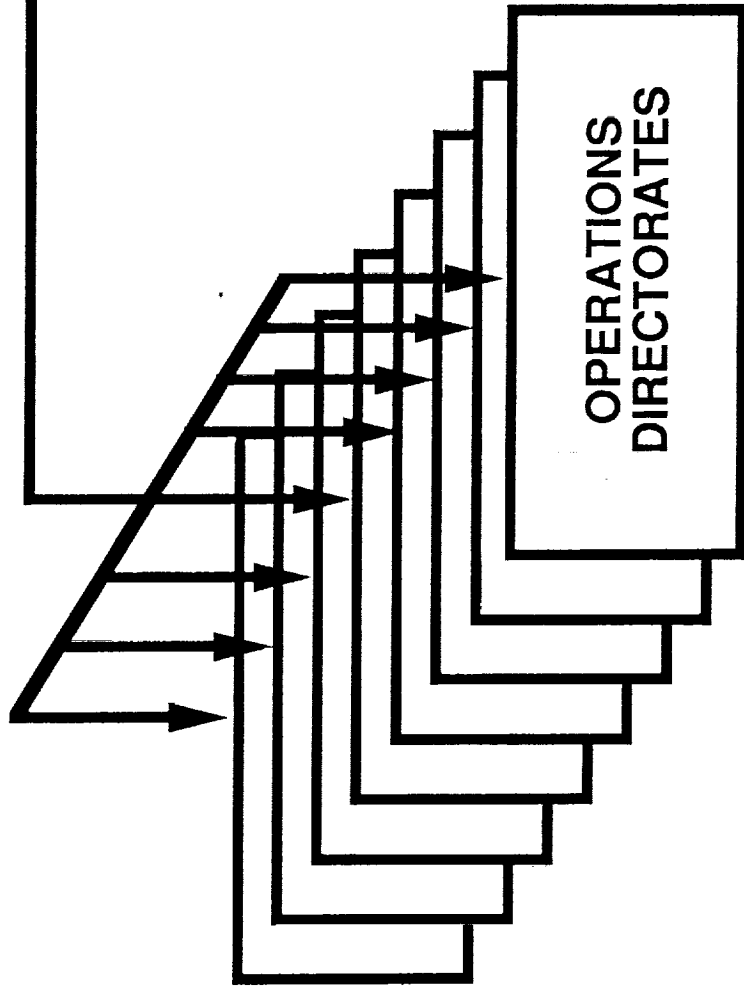
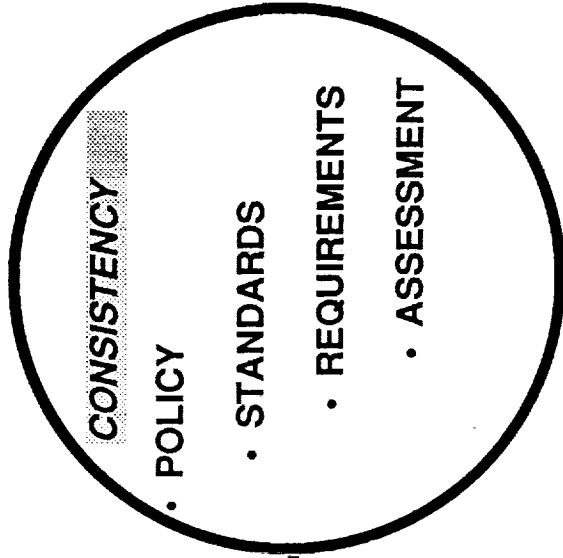
FUTURE CHALLENGES

EXISTING POLICIES & GUIDELINES



FUTURE CHALLENGES

NEEDED POLICY & GUIDELINES



BOTTOM LINE

THE KEY TO COST EFFECTIVE AIS
SECURITY IS THE PROPER
APPLICATION OF RISK MANAGEMENT
AND...

TECHNOLOGY

~~PAGE INTENTIONALLY BLANK~~