

# **Auditing for Database Systems and Applications**

**Marvin Schaefer**  
**Arca Systems, Inc.**

**CMAD IV Workshop**  
**November 12-14, 1996**

# Audit Goals

- ✦ **Accurately Record Events**
  - **Protection Critical**
    - Policy-Based
    - Who, What, When
  - **Integrity Critical**
    - Transaction-Based
    - Who, What, When, Why
  - **Private**
    - from normal users, applications
    - from “outsiders”
  - **Protected**
    - from unauthorized users

# Levels of Abstraction

- ✧ **User**
  - **Intention?**
- ✧ **Application**
  - **HOL Expression**
  - **Compiled Expression**
    - **Optimisation**
- ✧ **Server**
  - **Input**
  - **Mediation**
  - **Result**
- ✧ **O/S - IDS**
  - **Gazintas**
  - **Gazoutes**

# Points of Confusion

- ✧ **OS/TCB excel in syntactic stuff**
  - **Does not address change in contents**
- ✧ **Applications excel in semantic richness**
  - **Does address internal content and structure**
- ✧ **OS/TCB relatively old, archaic, stable, planned**
- ✧ **Applications often flexible, up-to-date, once planned, intuitive or hopeful**
  - **Maintenance & planning vs \$49 update**