Federal Information System Controls Audit Manual (FISCAM)

Presented at CSSPAB's Workshop on Approaches to Measuring Security

June13, 2000

GAO

Agenda

- Overview of FISCAM
  - Focus on Chapter 3-General Controls
- Computer Controls
  - Significance
  - Audit Results
- Penetration Testing

GAO

Significance of Information Security Audits

- Increasingly important aspect of control over critical operations, assets, and data
- Legislation calls for improvements in systems and internal controls
- GAO High-Risk Area - Problems identified in all 24 CFO agencies
- Increased Congressional interest
- Government Information Security Act of 1999

Increased Inherent Risks

- Dollars passing through automated systems are rising
- Speed and accessibility
- Increased computer skills
- Availability of hacking tools
- Reduced paper backup
- More reliance on computer controls
- Trend toward providing broad access

Information System Risks

- Modification or destruction of data
- Loss of Assets
- Release of sensitive information (taxes, social security, medical records, other)
- Disruption of critical operations

GAO

FISCAM - Purpose

- At first, developed to support our financial statement audits

- Now, is also used during non-financial audits

- Describes elements of a full-scope information security audit from which auditor can select elements that support job objectives

FISCAM - Organization of Manual

- Chapter 1 - Introduction and General Methodology
- Chapter 2 - Planning the Audit
- Chapter 3 - Evaluating and Testing General Controls
- Chapter 4 - Evaluating and Testing Application Controls
- Appendixes

GAO

FISCAM - Chapters 3 and 4

- Describe broad control areas; provide criteria
- Identify critical elements of each control area
- List common types of control techniques
- List suggested audit procedures

Chapter 3 - Evaluating and Testing General Controls

Six general control areas covered

- Entitywide Security Program Planning and Management (SP)
- Access Control (AC)
- Application Software Development and Change Control (CC)
- System Software (SS)
- Segregation of Duties (SD)
- Service Continuity (SC)

Critical Elements - Entitywide Security Program

- Assess risks
- Document plan
- Establish management structure; assign responsibilities
- Implement personnel policies
- Monitor program’s effectiveness

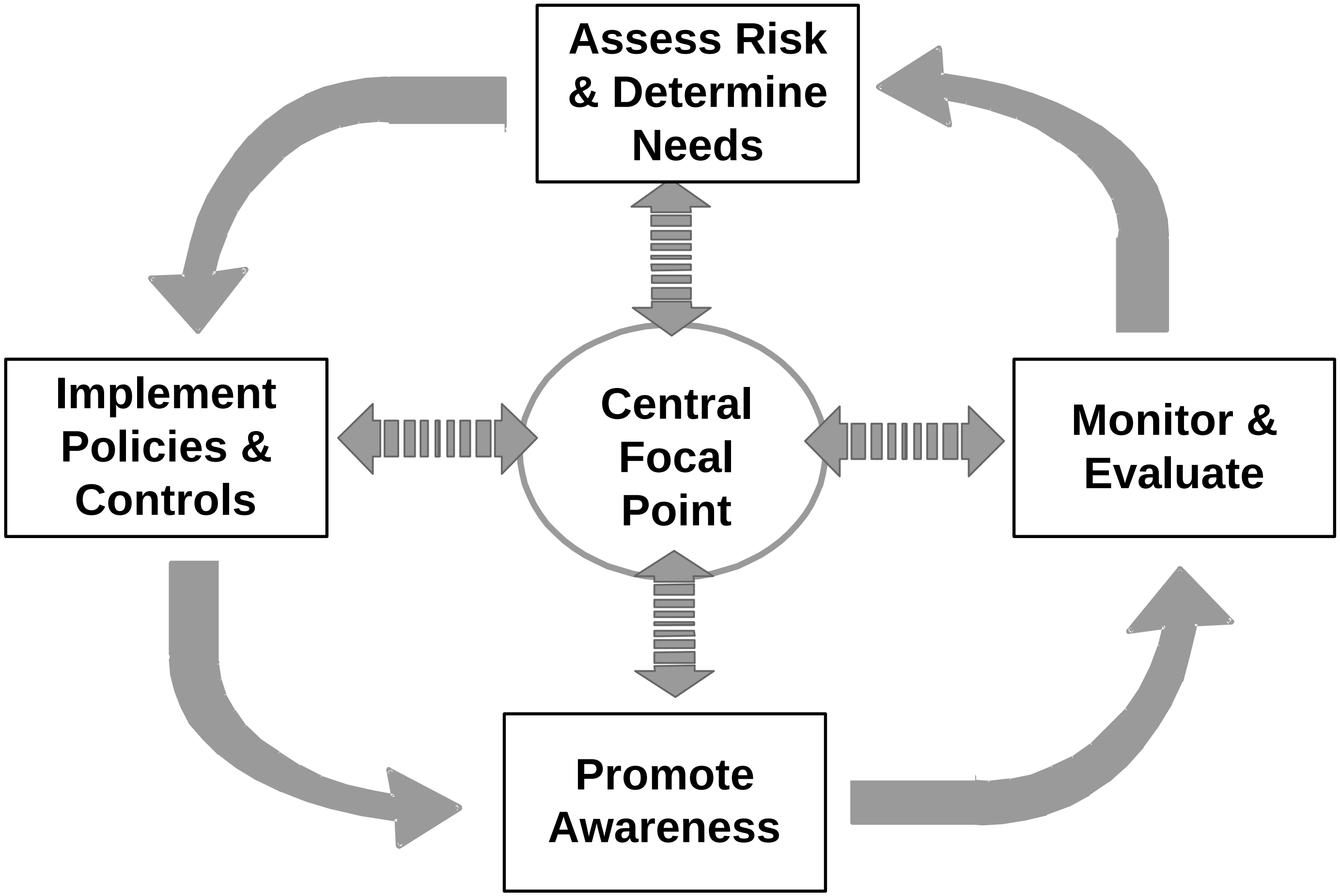
Best Practices

Information Security Management:
Learning from Leading Organizations
(GAO/AIMD-98-68)

- Addresses an underlying cause of ineffective security controls
- Supplements FISCAM information on security program planning and management
- Final guide issued in May 1998

GAO

Risk Management Cycle



Assess Risk & Determine Needs

Implement Policies & Controls

Central Focal Point

Monitor & Evaluate

Promote Awareness

GAO

Entitywide Security Program - Audit Results

- Weaknesses at all agencies reviewed
    - No risk-based security plans
    - Undocumented policies
    - Inadequate monitoring program
    - Lack of coordinated security function

Critical Elements - Access Controls

- Classify resources by criticality and sensitivity
- Identify authorized users and access authorized
- Establish physical and logical controls
- Monitor access, investigate violations, and take action

Access Controls - Audit Results

- Most widely reported problem area
  - Overly broad access, not periodically reviewed
  - Undocumented access granted
  - Poor id and password management
  - Improper implementation of software controls
  - Inadequate monitoring of user activity

Critical Elements - Application Software Development and Change Control

- Programs and modifications are authorized
- Test and approve all new and revised software
- Control software libraries

Application Development and Change Control - Audit Results

- Undisciplined testing procedures
- Unauthorized software and software changes
- Inappropriate access to software

Critical Elements - System Software

- Limit access to system software
- Monitor access to and use of system software
- Control system software changes

GAO

System Software - Audit Results

- Inadequately controlled access to powerful system software
- Inadequate monitoring of authorized users

Critical Elements - Segregation of Duties

- Segregate incompatible duties and establish related policies
- Establish access controls to enforce segregation of duties
- Control activities through operating procedures and supervision and review

Segregation of Duties - Audit Results

- Excessive responsibilities
  - Develop, test, review, and approve software changes
  - Perform all steps needed to initiate and complete a payment

GAO

Critical Elements - Service Continuity

- Assess criticality of operations and identify supporting resources
- Take steps to prevent and minimize potential damage and interruption
- Develop and document a comprehensive contingency plan
- Periodically test plan and adjust as appropriate

GAO

Service Continuity - Audit Results

- Incomplete plans
- Incomplete testing

GAO

Example of Control Activities/Techniques and Audit Procedures

Control Activities	Control Techniques	Audit Procedures
SP-3.3 Owners and users are aware of security policies	An ongoing security awareness program has been implemented. It includes first-time training for all new employees, contractors, and users, and periodic refresher training thereafter. Security policies are distributed to all affected personnel, including system/application rules and expected behaviors.	Review documentation supporting or evaluating the awareness program. Observe a security briefing. Interview data owners and system users. Determine what training they have received and if they are aware of their security-related responsibilities. Review memos, electronic mail files, or other policy distribution mechanisms. Review personnel files to test whether security awareness statements are current.

Example of Control Activities/Techniques and Audit Procedures

Control Activities	Control Techniques	Audit Procedures
AC-2.1 Resource owners have identified authorized users and their access authorized	Access authorizations are --documented on standard forms and maintained on file --approved by senior managers --securely transferred to security managers Owners periodically review access authorization listings and determine whether they remain appropriate	Review policies and procedures. For a selection of users, review access authorization documentation. Interview owners and review supporting documentation.

Chapter 4 - Application Controls

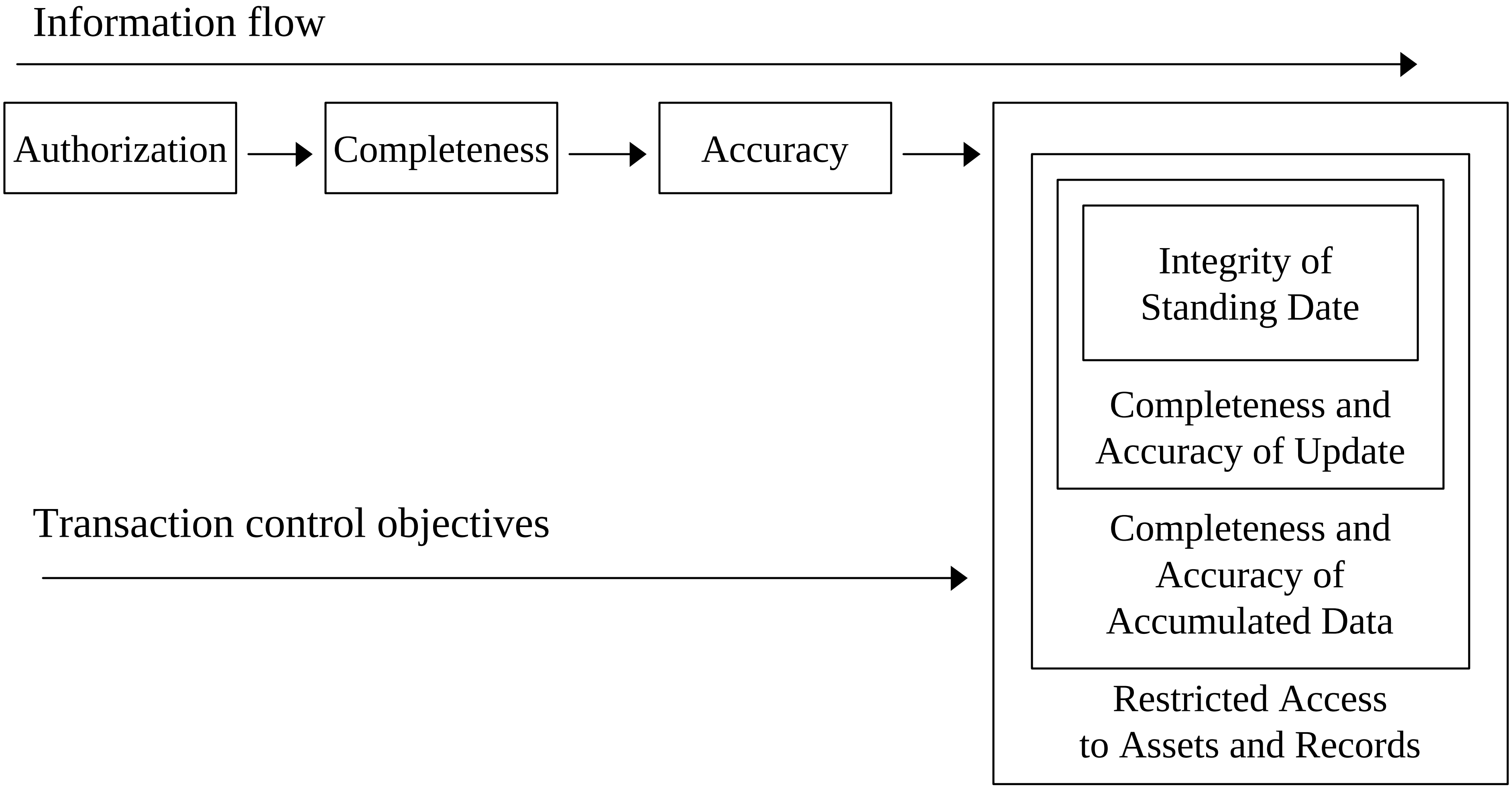
- Apply to the processing of individual applications

- Designed to ensure that transactions are
  - valid
  - properly authorized
  - completely and accurately processed

GAO

CONTROLS OVER APPLICATIONS

Overview of Objectives to Consider



Information flow

Authorization → Completeness → Accuracy →

Integrity of Standing Date

Completeness and Accuracy of Update

Completeness and Accuracy of Accumulated Data

Restricted Access to Assets and Records

Transaction control objectives

Application controls consist of:

- Initial controls related to the control of information prior to system input
- Programmed controls, such as edits, and
- Manual follow-up of EDP produced reports, such as exception reports or reconciliations

GAO

Critical Elements - Authorization Controls

- All data are authorized before entering the application system
- Restrict data entry terminals to authorized users for authorized purposes
- Master files and exception reporting help ensure all data processed are authorized

Critical Elements - Completeness Controls

- All authorized transactions are entered into and processed by the computer
- Reconciliations are performed to verify data completeness

GAO

Critical Elements - Accuracy Controls

- Data entry design features contribute to data accuracy
- Data validation and editing are performed to identify erroneous data
- Erroneous data are captured, reported, investigated, and corrected
- Review of output helps to maintain data accuracy and validity

GAO

Application Controls -
Common Control Techniques

- Authorization routines
- Segregation of duties
- Computer matching
- Computer sequence check
- Agreement of batch totals
- One for One checking
- Edit checks
- Reconciliations of file totals
- Exception reporting
- Detailed file data checks
- Data access security controls
- Physical access controls

FISCAM Appendices

- Questionnaires on background information and user satisfaction
- Tables for summarizing work performed and assessment of control effectiveness
- Knowledge, skills and abilities
- Audit planning strategy
- Glossary
- Principles for managing an information security program

Penetration Testing

Using automated tools and techniques to identify security exposures from internal and external threats

GAO Position

- Use penetration as part of all general control reviews
- Use penetration testing in selected sensitive areas
- Encourage Inspectors General to use

Targets

Sensitive Applications and Data

Tier I Systems	Mainframe
Tier II Systems	Minicomputer
Tier III Systems	Network Systems

Targets (cont.)

Platforms	Examples
Mainframe	MVS, VM, Unisys ...
Minicomputer	Unix, VMS, AS/400 ...
Network	Windows NT, NetWare, Firewalls, Web, Proxy & Mail Servers, Routers, Hubs, Dial-in Modems ...

Test Scenarios

Scenario	Facility Info	Physical Access	Logical Access	Test Paths	Test Type
Outsider	Little or None	No	No	-Dial-In -Internet	Hacker or Cyber-Terrorist
Outsider	Medium to High	No	No	-Dial-In -Internet	Former employee, contractor or temp
Insider	Medium	Yes	No	-Unused connections -Unattended workstations	Disgruntled or dishonest employee, contractor or temp
Insider	High	Yes	Yes	-Work-stations -WAN	Disgruntled or dishonest employee, contractor or temp

Planning

Terms of Engagement

- Define Scope
- Address Risks
- Identify Roles and Responsibilities
- Determine Logistical Requirements

Terms of Engagement
Define Scope

Test Parameters

• What	What is to be tested?
• When	Timeframe Stopping Points
• Where	From what locations?
• Who	Who will perform testing?
• How	What tools & techniques?

Terms of Engagement Address Risks

- Risks cannot be eliminated but must be minimized to an acceptable level

- Acceptance of risks by System Owners

Terms of Engagement Address Risks (cont.)

Steps to Minimize Risks

- No Denial of Service
- Coordinate Testing
- Have Knowledgeable Site Personnel Monitor All Testing
- Log Test Settings
- Maintain Detailed Log of All Tests & Results
- Use Network Analyzers
- Test During Non-Peak Hours (if necessary)

GAO

Terms of Engagement
Define Roles & Responsibilities

Participants

- Contractors
- Test Team
- EDP Auditors
- System Owners (CIO & Functional Area Mgr.)
- Security Officer
- System Administrators

Terms of Engagement
Identify Logistical Requirements

- IP Addresses
- Telephone Ranges (exclude sensitive no.'s)
- Control of Sensitive Information
- Secure Workspace
- Analog Telephone Lines
- Internet Access
- User Accounts and Passwords
- Levels of Access
- Network Connections
- IP Assignment
- Workstations

GAO

Tools and Techniques

Internet Available Tools and Information

- Freeware
- Shareware
- Commercial Software

GAO

Tools and Techniques

- Data Gathering

  whois, finger, ping, traceroute, Web pages, phone book, …
- Scanning

  Port Scanners - ISS, CyberCop Scanner, …

  Modem Dialers - ToneLoc, Phonetag, …
- Data Extraction, Analysis & Testing

  Standard OS commands and utilities

  Automated Tools - DumpACL, CA-Examine, NetXRay, Keycopy …
- Password Cracking

  L0phtCrack (NT), John the Ripper (Unix), Pandora (Novell), …
- Social Engineering

  Help desk, employees, contractors, temps …

Common Vulnerabilities

- Weak Passwords
- Default Accounts and Passwords Not Changed
- Repeated Bad Logon Attempts Allowed
- No Real-Time Intrusion Detection Capability
- Unpatched, Outdated Vulnerable Services
- Running Unnecessary Services
- Misconfigured File Sharing Services
- Inappropriate File Permissions
- Excessive Admin & User Rights

Common Vulnerabilities (cont.)

- Clear Text transmissions of Sensitive Information
- Unsecured Dial-In Modems
- Inadequate Filtering
- Inadequate Logging, Monitoring & Detection
- Excessive Trust Relationships
- Information Leakage
- Inadequate Segregation of Duties
- Inadequate Warning Banners

GAO

Available on GAO’s Internet Web Site **<http://www.gao.gov>**

- FISCAM (GAO/AIMD-12.19.6, January 1999)
- Information Security: Serious Weakness Place Critical Federal Operations and Assets at Risk (GAO/AIMD-98-92, September 1998)
- (GAO/AIMD-99-227, July 1999)
- (GAO/AIMD-98-175, September 1998)
- (GAO/AIMD-99-10, October 1998)

GAO

Contacts

- **FISCAM**

Darrell Heim	(202) 512-6237
Jean Boltz	(202) 512-5247

- **Penetration Testing**

Ed Glagola	(202) 512-6270
Lon Chin	(202) 512-2842

- **Best Practices**

Jean Boltz	(202) 512-5247

Questions and Answers