INFORMATION TECHNOLOGY AUDITING

GAO AND THE FISCAM AUDIT FRAMEWORK

Presented by

Ronald E. Franke, CISA, CIA, CFE, CICA

Clifton Gunderson LLP
Certified Public Accountants & Consultants

Count on Insight™

April 30, 2010

1

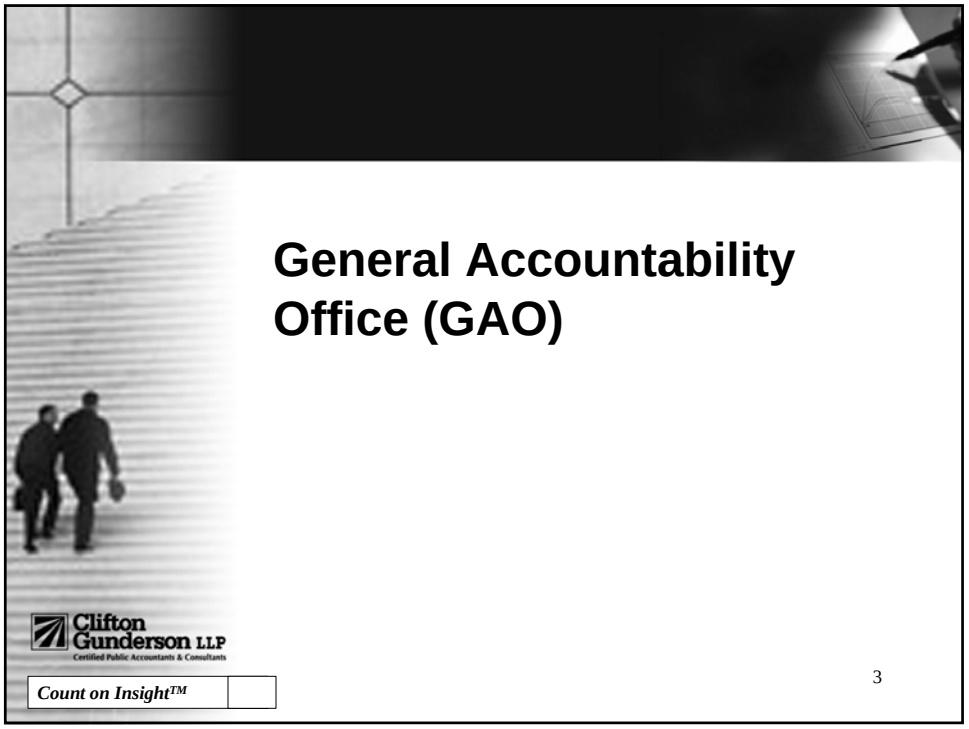
Agenda

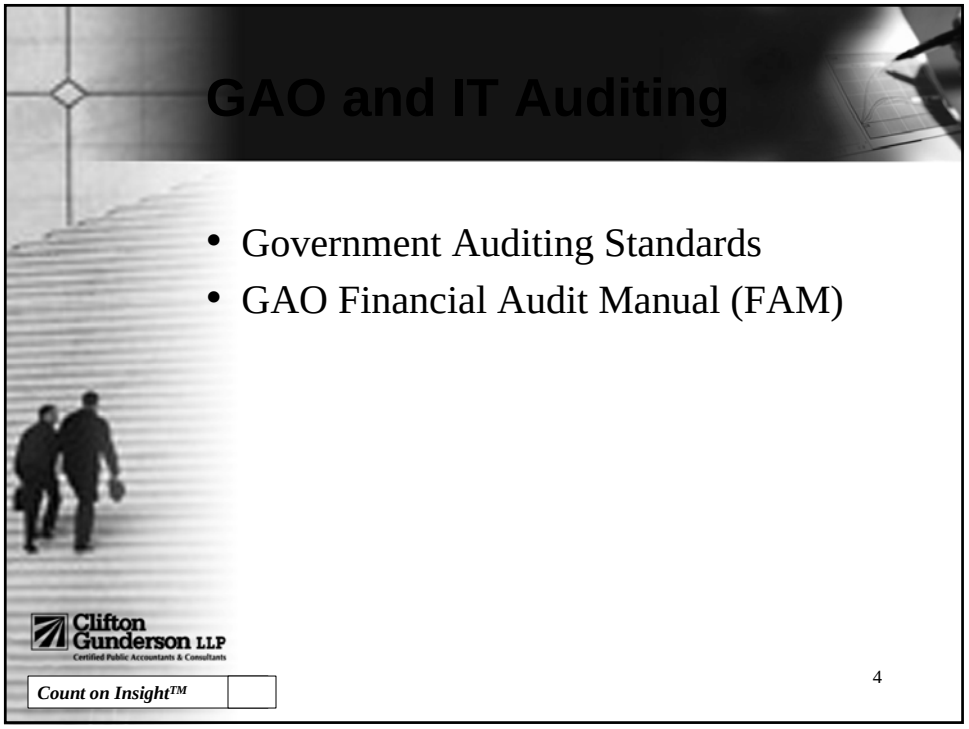
- General Accountability Office (GAO) and IT Auditing
- Federal Information System Controls Audit Manual (FISCAM)

Clifton Gunderson LLP
Certified Public Accountants & Consultants

Count on Insight™

2


General Accountability Office (GAO)
Clifton Gunderson LLP
Certified Public Accountants & Consultants
Count on Insight™
3


GAO and IT Auditing
• Government Auditing Standards
• GAO Financial Audit Manual (FAM)
Clifton Gunderson LLP
Certified Public Accountants & Consultants
Count on Insight™
4

Government Auditing Standards ("Yellow Book")

- Revised July 2007
- Effective for financial and attestation engagements for periods beginning on or after January 1, 2008
- Effective for performance audits beginning on or after January 1, 2008
- http://www.gao.gov/govaud/ybk01.htm

Clifton Gunderson LLP
Certified Public Accountants & Consultants

Count on Insight™

5

GAS – Major Changes

- Standardized language to define the auditor's level of responsibility and distinguish between requirements and guidance/explanatory material.
- Recognizes that other sets of professional standards can be used in conjunction with GAGAS.
- Clarified discussion of nonaudit services and their impact on auditor independence
- Incorporated the revised CPE requirements that were issued by GAO in April 2005
- Clarified Quality Control and Assurance requirements

Clifton Gunderson LLP
Certified Public Accountants & Consultants

Count on Insight™

6

GAS – Major Changes

- Added/clarified reporting guidance.
- Updated financial auditing standards based on recent developments from AICPA (SAS 103 & SAS 112).
- Clarified/Revised definition of Performance Audits and enhanced performance auditing standards.
- Clarified auditors' responsibilities for internal control based on significance to the audit objectives.
- **Added a section on information systems controls for the purpose of assessing audit risk and planning the audit.**

Clifton Gunderson LLP
Certified Public Accountants & Consultants

Count on Insight™

7

GAO Financial Audit Manual

- In July 2001 the GAO and the President's Council on Integrity and Efficiency (PCIE) jointly issued the *GAO/PCIE Financial Audit Manual* (FAM).
- The FAM presents a methodology to perform financial statement audits of federal entities in accordance with professional standards.
- Updated July 2008 for significant changes that have occurred in auditing financial statements in the federal government.

Clifton Gunderson LLP
Certified Public Accountants & Consultants

Count on Insight™

8

GAO – FAM (Volume 1)

- Section 100 - Table of Contents, Introduction
- Section 200 - Planning
- Section 300 - Internal Control
- Section 400 - Testing
- Section 500 – Reporting
- Section Appendixes - Appendixes, Glossary, Abbreviations, Index

Clifton Gunderson LLP
Certified Public Accountants & Consultants

Count on Insight™

9

GAO – FAM (Volume 2)

- Section 600 - Planning and General
- Section 700 - Internal Control
- Section 800 - Compliance
- Section 900 - Substantive Testing
- Section 1000 - Reporting

Clifton Gunderson LLP
Certified Public Accountants & Consultants

Count on Insight™

10

GAO – FAM (Volume 3)

- FAM 2010, *Checklist for Federal Accounting*
- FAM 2020, *Checklist for Federal Reporting and Disclosures*
- Checklists issued to assist:
  - Federal entities in preparing their financial statements in accordance with U.S. GAAP
  - Auditors in auditing them in accordance with U.S. generally accepted government auditing standards (GAGAS)

Clifton Gunderson LLP
Certified Public Accountants & Consultants

Count on Insight™

11

Federal Financial Management Improvement Act of 1996 (FFMIA)

- "Each audit…shall report whether the agency financial management reporting systems…comply substantially with…the act's three requirements."
  - Federal financial management system requirements
  - Federal accounting standards
  - *US Government Standard General Ledger* (SGL) at the transaction level

Clifton Gunderson LLP
Certified Public Accountants & Consultants

Count on Insight™

12

FFMIA and OMB Cir A-127

- OMB Circular A-127, *Financial Management Systems*
- Includes the Joint Financial Management Improvement Program's series of system requirements documents

Clifton Gunderson LLP
Certified Public Accountants & Consultants

Count on Insight™

13

Federal Information System Controls Audit Manual (FISCAM)

Clifton Gunderson LLP
Certified Public Accountants & Consultants

Count on Insight™

14

Increased Inherent Risks

- Dollars passing through automated systems increasing
- Speed and accessibility of processing
- Increased computer skills and availability of hacking tools
- Reduced paper backup
- More reliance on computer controls
- Trend toward providing broad access including web-based systems and applications
- Remote/telecommuting and mobile devices
- Inter-relations of systems
- Outsourcing and use of service providers

Clifton Gunderson LLP
Certified Public Accountants & Consultants

Count on Insight™

15

Information System Risks

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

Clifton Gunderson LLP
Certified Public Accountants & Consultants

Count on Insight™

16

Assess IT Controls - Inherent Risks

- Uniform processing of transactions
- Automatic processing
- Increased potential for undetected misstatements
- Existence, completeness, and volume of the audit trail
- Nature of the hardware and software
- Unusual or non-routine transactions

Clifton Gunderson LLP
Certified Public Accountants & Consultants

Count on Insight™

17

Impact of Inherent Risk and Control Environment on Audits

- Assessed Risk
- Identify Effective IT-Related Controls
- Substantive Testing

Clifton Gunderson LLP
Certified Public Accountants & Consultants

Count on Insight™

18

FISCAM - Purpose

- At first, developed to support Chief Financial Officer Act financial statement audits
- Now, is also used during non-financial audits
- Describes elements of a full-scope information system controls audit from which auditor can select elements that support audit objectives

Clifton Gunderson LLP
Certified Public Accountants & Consultants

Count on Insight™

19

FISCAM – Recent Revisions

- GAO Report Number GAO-09-232G
- Released February 2, 2009
- http://www.gao.gov/special.pubs/fiscam.html

Clifton Gunderson LLP
Certified Public Accountants & Consultants

Count on Insight™

20

FISCAM – Recent Revisions

- Reflects changes in:
  - Technology used by government entities
  - Audit guidance and control criteria issued by NIST
  - GAGAS
- Provides a methodology for performing information system control audits in accordance with GAGAS, where IS controls are significant to the audit objectives.
- Conformity with AICPA auditing standards, including new risk standards.
- An overall framework of IS control objectives

Clifton Gunderson LLP
Certified Public Accountants & Consultants

Count on Insight™

21

FISCAM – Recent Revisions

- IS controls audit documentation guidance for each audit phase
- Additional audit considerations that may affect an IS audit, including:
  - information security risk factors
  - automated audit tools
  - sampling techniques
- Audit methodology and IS controls for business process applications that (1) are consistent with GAGAS and current NIST and OMB information security guidance (particularly NIST Special Publication 800-53) including references/mapping to such guidance

Clifton Gunderson LLP
Certified Public Accountants & Consultants

Count on Insight™

22

FISCAM – Recent Revisions

Expanded appendices to support IS audits:

- Updated IS controls audit planning checklist
- Tables for summarizing results of the IS audit
- Mapping of FISCAM to NIST SP 800-53
- Knowledge, skills, and abilities needed to perform IS audits
- Scope of an IS audit in support of a financial audit
- Entity's use of service organizations
- Application of FISCAM to Single Audits
- Application of FISCAM to FISMA
- IS Controls Audit Documentation

Clifton Gunderson LLP
Certified Public Accountants & Consultants

Count on Insight™

23

FISCAM Overview

- FISCAM presents a methodology for performing information system (IS) control audits of federal and other governmental entities in accordance with professional standards.
- The FISCAM is designed to be used primarily on financial and performance audits and attestation engagements performed in accordance with GAGAS, as presented in *Government Auditing Standards* ("Yellow Book").
- The FISCAM is consistent with the *GAO/PCIE Financial Audit Manual* (FAM).
- FISCAM control activities are consistent with NIST Special Publication 800-53, and all SP800-53 controls have been mapped to the FISCAM.

Clifton Gunderson LLP
Certified Public Accountants & Consultants

Count on Insight™

24

FISCAM Overview

Organized to facilitate effective and efficient IS control audits:

- Top-down, risk based approach that considers materiality and significance in determining effective and efficient audit procedures and is tailored to achieve the audit objectives.
- Evaluation of entitywide controls and their effect on audit risk.
- Evaluation of general controls and their pervasive impact on business process application controls.
- Evaluation of security management at all levels.
- A control hierarchy (control categories, critical elements, and control activities) to assist in evaluating the significance of identified IS control weaknesses.
- Groupings of control categories consistent with the nature of the risk.
- Experience gained in GAO's performance and review of IS control audits.

Clifton Gunderson LLP
Certified Public Accountants & Consultants

Count on Insight™

25

FISCAM - Organization of Manual

- Chapter 1 - Introduction and General Methodology
- Chapter 2 - Performing the Information System Controls Audit
- Chapter 3 - Evaluating and Testing General Controls
- Chapter 4 - Evaluating and Testing Business Process Application Controls
- Appendices

Clifton Gunderson LLP
Certified Public Accountants & Consultants

Count on Insight™

26

FISCAM - Chapters 1 and 2

- Plan the Information System Controls Audit:
  - Understand the Overall Audit Objectives and Related Scope of the Information System Controls Audit.
  - Understand the Entity's Operations and Key Business Processes.
  - Obtain a General Understanding of the Structure of the Entity's Networks.
  - Identify Key Areas of Audit Interest.
  - Assess Information System Risk on a Preliminary Basis.
  - Identify Critical Control Points.
  - Obtain a Preliminary Understanding of Information System Controls.

Clifton Gunderson LLP
Certified Public Accountants & Consultants

Count on Insight™

27

FISCAM - Chapters 1 and 2

- Perform Other Audit Planning Procedures;
  - Relevant Laws and Regulations;
  - Consideration of the Risk of Fraud;
  - Audit Resources;
  - Multiyear Testing Plans;
  - Communication with Entity Management and Those Charged with Governance;
  - Service Organizations;
  - Using the Work of Others;
  - Audit Plan.

Clifton Gunderson LLP
Certified Public Accountants & Consultants

Count on Insight™

28

FISCAM - Chapters 1 and 2

- Perform Information System Controls Audit Tests:
  - Understand Information Systems Relevant to the Audit Objectives.
  - Determine which IS Control Techniques are Relevant to the Audit Objectives.
  - For each Relevant IS Control Technique Determine Whether it is Suitably Designed to Achieve the Critical Activity and has been Implemented.
  - Perform Tests to Determine Whether such Control Techniques are Operating Effectively.
  - Identify Potential Weaknesses in IS Controls and Consider Compensating Controls.

Clifton Gunderson LLP
Certified Public Accountants & Consultants

Count on Insight™

29

FISCAM - Chapters 1 and 2

- Report Audit Results:
  - Evaluate the Effects of Identified IS Control Weaknesses: - Financial Audits, Attestation Engagements, and Performance Audits.
  - Consider Other Audit Reporting Requirements and Related Reporting Responsibilities.

Clifton Gunderson LLP
Certified Public Accountants & Consultants

Count on Insight™

30

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

Clifton Gunderson LLP
Certified Public Accountants & Consultants

Count on Insight™

31

Chapter 3 - Evaluating and Testing General Controls

Five general control areas covered

- Security Management (SM)
- Access Controls (AC)
- Configuration Management (CM)
- Segregation of Duties (SD)
- Contingency Planning (CP)

Clifton Gunderson LLP
Certified Public Accountants & Consultants

Count on Insight™

32

Critical Elements - Security Management

- Controls provide reasonable assurance that security management is effective, including effective:
  - security management program
  - periodic assessments and validation of risk
  - security control policies and procedures
  - security awareness training and other security-related personnel issues
  - periodic testing and evaluation of the effectiveness of information security policies, procedures, and practices
  - remediation of information security weaknesses
  - security over activities performed by external third parties.

Clifton Gunderson LLP
Certified Public Accountants & Consultants

Count on Insight™

33

Security Management -Audit Results

- No risk-based security plans
- No or inadequate risk assessment
- Undocumented policies
- Inadequate monitoring program
- Lack of coordinated security function
- Lack of or weak awareness training or lack of documentation

Clifton Gunderson LLP
Certified Public Accountants & Consultants

Count on Insight™

34

Critical Elements -Access Controls

- Controls provide reasonable assurance that access to computer resources (data, equipment, and facilities) is reasonable and restricted to authorized individuals, including effective:
  - protection of information system boundaries
  - identification and authentication mechanisms
  - authorization controls
  - protection of sensitive system resources
  - audit and monitoring capability, including incident handling
  - physical security controls

Clifton Gunderson LLP
Certified Public Accountants & Consultants

Count on Insight™

35

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

Clifton Gunderson LLP
Certified Public Accountants & Consultants

Count on Insight™

36

GAO Summary of Security – Audit Results

- GAO found that out of 24 major agencies:
  - Thirteen said controls over financial systems and information were a "significant deficiency" and seven said it was a "material weakness" in performance and accountability reports for fiscal 2008.
  - Twenty-two of the agencies' IGs identified information security as a "major management challenge" for their agency.
  - Twenty-three had weaknesses in access controls reported and 23 had weaknesses in their agencywide information security programs.

Clifton Gunderson LLP
Certified Public Accountants & Consultants

Count on Insight™

37

Critical Elements – Configuration Management

- Controls provide reasonable assurance that changes to information system resources are authorized and systems are configured and operated securely and as intended, including effective:
  - configuration management policies, plans, and procedures
  - current configuration identification information
  - proper authorization, testing, approval, and tracking of all configuration changes
  - routine monitoring of the configuration
  - updating software on a timely basis to protect against known vulnerabilities
  - documentation and approval of emergency changes to the configuration

Clifton Gunderson LLP
Certified Public Accountants & Consultants

Count on Insight™

38

Configuration Management - Audit Results

- Undisciplined testing procedures
- Unauthorized software and software changes
- Lack of documentation
- Inappropriate access to software

Clifton Gunderson LLP
Certified Public Accountants & Consultants

Count on Insight™

39

Critical Elements - Segregation of Duties

- Controls provide reasonable assurance that incompatible duties are effectively segregated, including effective
  - segregation of incompatible duties and responsibilities and related policies
  - control of personnel activities through formal operating procedures, supervision, and review

Clifton Gunderson LLP
Certified Public Accountants & Consultants

Count on Insight™

40

Segregation of Duties - Audit Results

- Excessive responsibilities
- Develop, test, review, and approve software changes
- Sharing of user, security management, DBA, system administrator functions
- Perform all steps needed to initiate and complete a payment

Clifton Gunderson LLP
Certified Public Accountants & Consultants

Count on Insight™

41

Critical Elements – Contingency Planning

- Controls provide reasonable assurance that contingency planning (1) protects information resources and minimizes the risk of unplanned interruptions and (2) provides for recovery of critical operations should interruptions occur, including effective
  - assessment of the criticality and sensitivity of computerized operations and identification of supporting resources
  - steps taken to prevent and minimize potential damage and interruption
  - comprehensive contingency plan
  - periodic testing of the contingency plan, with appropriate adjustments to the plan based on the testing

Clifton Gunderson LLP
Certified Public Accountants & Consultants

Count on Insight™

42

Contingency Planning - Audit Results

- Incomplete plans
- Incomplete testing
- Weaknesses in backup and recovery procedures

Clifton Gunderson LLP
Certified Public Accountants & Consultants

Count on Insight™

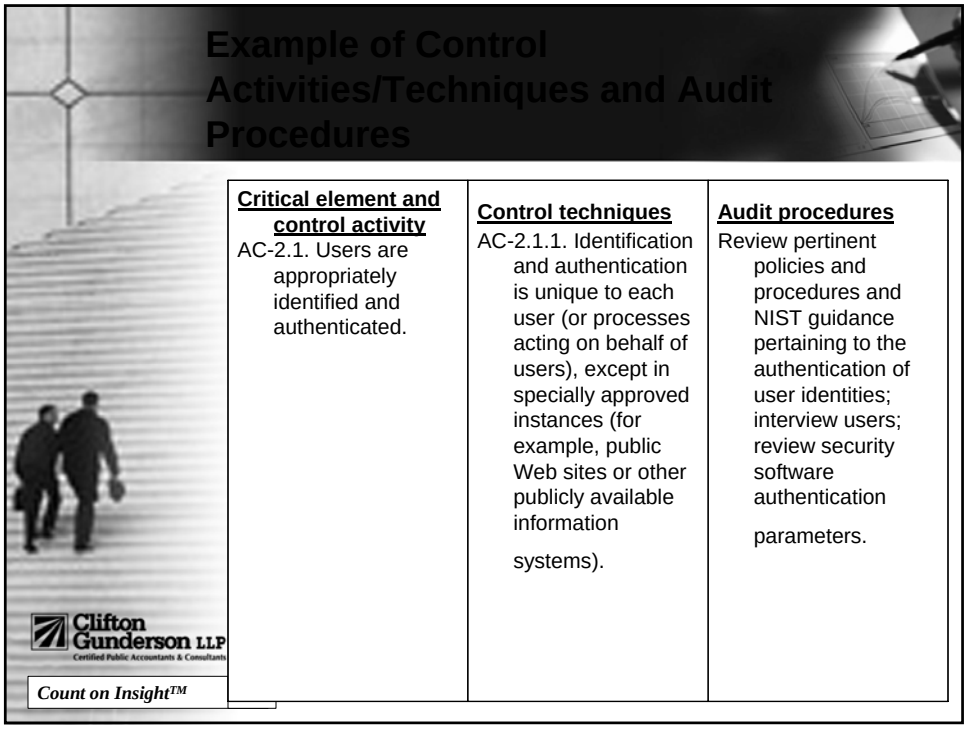
43

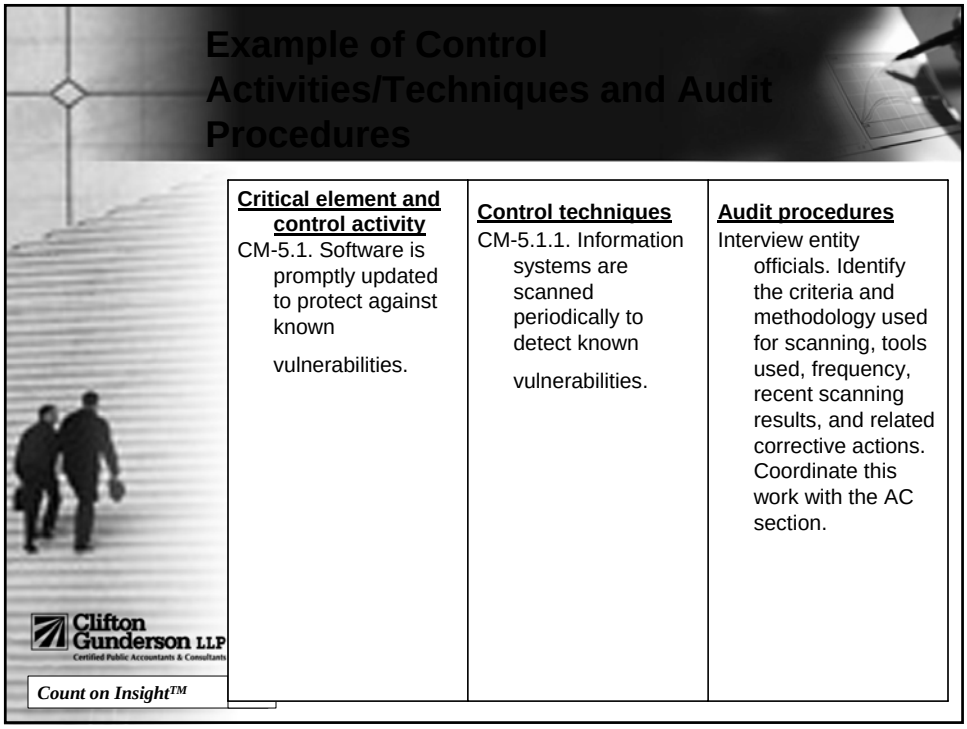
Example of Control Activities/Techniques and Audit Procedures

Critical element and control activity	**Control techniques**	**Audit procedures**
SM-1.2. A security management structure has been established.	SM-1.2.1. Senior management establishes a security management structure for the entitywide, system, and application levels that have adequate independence, authority, expertise, and resources.	Review security policies and plans, the entity's organization chart, and budget documentation. Interview security management staff. Evaluate the security structure: independence, authority, expertise, and allocation of resources required to adequately protect the information systems.

Clifton Gunderson LLP
Certified Public Accountants & Consultants

Count on Insight™


Example of Control Activities/Techniques and Audit Procedures
Critical element and control activity
AC-2.1. Users are appropriately identified and authenticated.
Control techniques
AC-2.1.1. Identification and authentication is unique to each user (or processes acting on behalf of users), except in specially approved instances (for example, public Web sites or other publicly available information systems).
Audit procedures
Review pertinent policies and procedures and NIST guidance pertaining to the authentication of user identities; interview users; review security software authentication parameters.
Clifton Gunderson LLP
Certified Public Accountants & Consultants
Count on Insight™


Example of Control Activities/Techniques and Audit Procedures
Critical element and control activity
CM-5.1. Software is promptly updated to protect against known vulnerabilities.
Control techniques
CM-5.1.1. Information systems are scanned periodically to detect known vulnerabilities.
Audit procedures
Interview entity officials. Identify the criteria and methodology used for scanning, tools used, frequency, recent scanning results, and related corrective actions. Coordinate this work with the AC section.
Clifton Gunderson LLP
Certified Public Accountants & Consultants
Count on Insight™

Chapter 4 – Evaluating and Testing Business Process Application Controls

- Apply to the processing of individual applications
- Designed to ensure that transactions are
  - valid
  - properly authorized
  - completely and accurately processed

Clifton Gunderson LLP
Certified Public Accountants & Consultants

Count on Insight™

47

Application controls consist of:

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

Clifton Gunderson LLP
Certified Public Accountants & Consultants

Count on Insight™

48

FISCAM Application Controls

- Application Level General Controls (AS)
- Business Process Controls (BP)
  - validity, completeness, accuracy, confidentiality of transactions and data during processing
- Interface Controls (IN)
  - timely, accurate and complete processing of information between systems
- Data Management Systems Controls (DA)
  - enter, store, retrieve or process information

Clifton Gunderson LLP
Certified Public Accountants & Consultants

Count on Insight™

49

Application Level General Controls – Critical Elements

- Implement effective application security management
- Implement effective application access controls
- Implement effective application configuration management
- Segregate user access to conflicting transactions and activities and monitor segregation
- Implement effective application contingency planning

Clifton Gunderson LLP
Certified Public Accountants & Consultants

Count on Insight™

50

Critical Elements –Application Level General 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

Clifton Gunderson LLP
Certified Public Accountants & Consultants

Count on Insight™

51

Critical Elements –Application Level General Controls

- Implement effective application security management.
- Implement effective application access controls.
- Implement effective application configuration management
- Segregate user access to conflicting transactions and activities and monitor segregation
- Implement effective application contingency planning

Clifton Gunderson LLP
Certified Public Accountants & Consultants

Count on Insight™

52

Chapter 4 – Evaluating and Testing Business Process Application Controls

- **Completeness** – controls provide reasonable assurance that all transactions that occurred are input into the system, accepted for processing, processed once and only once by the system, and properly included in output.
- **Accuracy** – controls provide reasonable assurance that transactions are properly recorded, with correct amount/data, and on a timely basis (in the proper period); key data elements input for transactions are accurate; data elements are processed accurately by applications that produce reliable results; and output is accurate.

Clifton Gunderson LLP
Certified Public Accountants & Consultants

Count on Insight™

53

Chapter 4 – Evaluating and Testing Business Process Application Controls

- **Validity** – controls provide reasonable assurance (1) that all recorded transactions and actually occurred (are real), relate to the organization, are authentic, and were properly approved in accordance with management's authorization; and (2) that output contains only valid data.
- **Confidentiality** – controls provide reasonable assurance that application data and reports and other output are protected against unauthorized access.
- **Availability** – controls provide reasonable assurance that application data and reports and other relevant business information are readily available to users when needed.

Clifton Gunderson LLP
Certified Public Accountants & Consultants

Count on Insight™

54

Critical Elements - Business Process Controls

- Transaction Data Input is complete, accurate, valid, and confidential (Transaction Data Input Controls)
- Transaction Data Processing is complete, accurate, valid, and confidential (Transaction Data Processing Controls)
- Transaction data output is complete, accurate, valid, and confidential (Transaction Data Output Controls)
- Master Data Setup and Maintenance is Adequately Controlled

Clifton Gunderson LLP
Certified Public Accountants & Consultants

Count on Insight™

55

Critical Elements - Interface Controls

- Implement an effective interface strategy and design.
- Implement effective interface processing procedures

Clifton Gunderson LLP
Certified Public Accountants & Consultants

Count on Insight™

56

Critical Elements - Data Management System Controls

- Implement an Effective Data Management System Strategy and Design

Clifton Gunderson LLP
Certified Public Accountants & Consultants

Count on Insight™

57

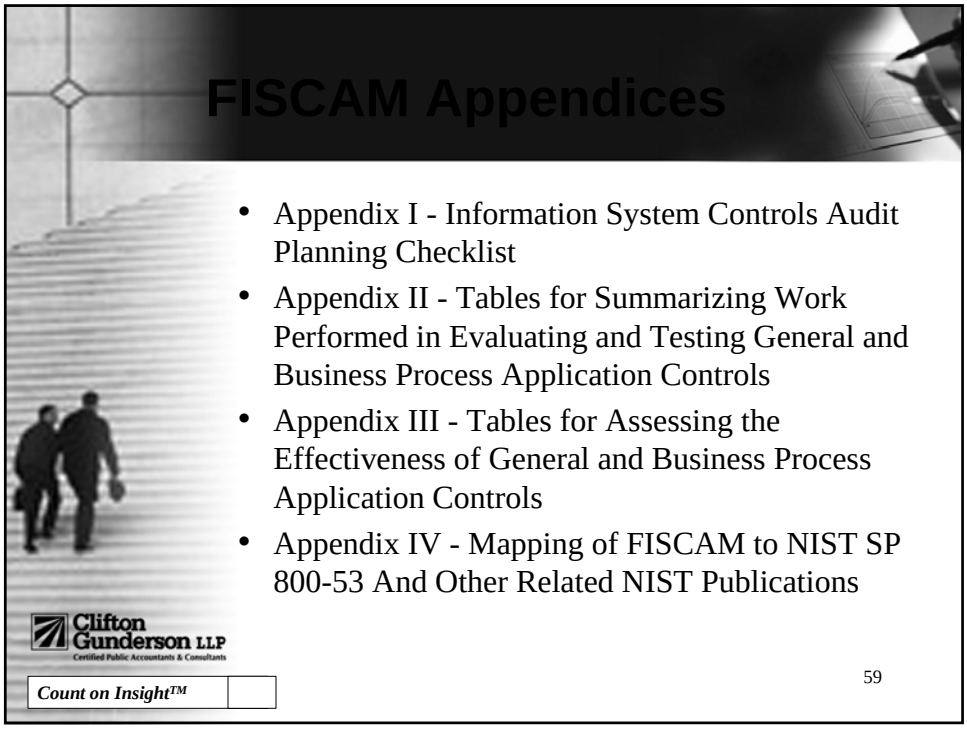
Application Controls - Common Control Techniques

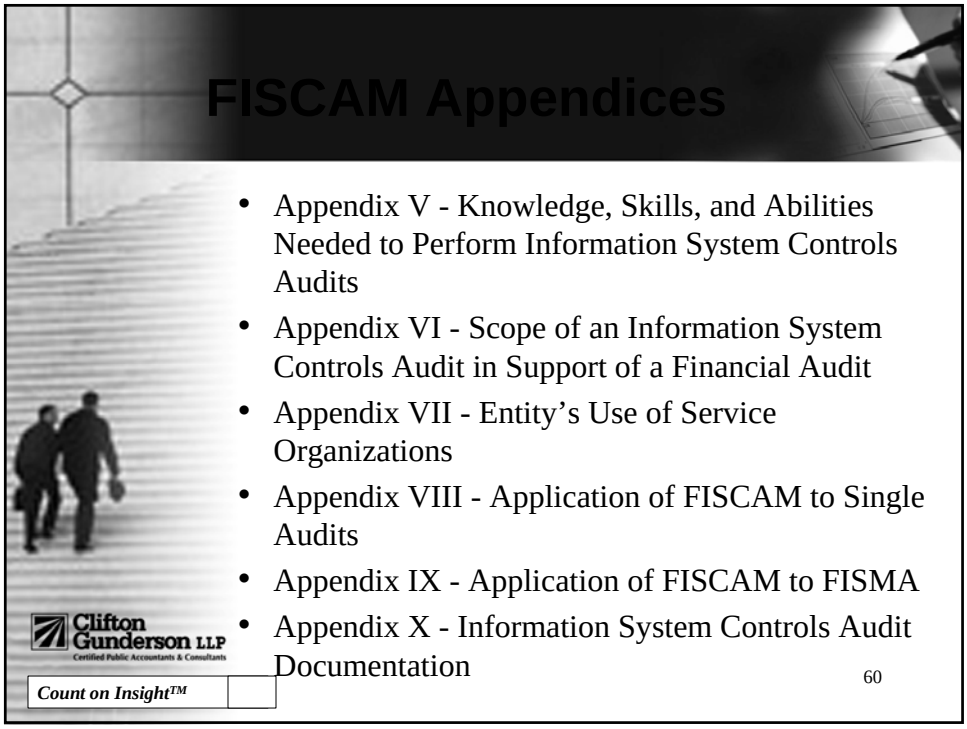
- Authorization routines
- Segregation of duties
- Computer matching
- Computer sequence check
- Agreement of batch totals
- One for One checking
- Edit checks
- Reconciliations of file totals
- Exception reporting
- Detailed file data checks
- Data access security controls
- Physical access controls

Clifton Gunderson LLP
Certified Public Accountants & Consultants

Count on Insight™

58


FISCAM Appendices
Appendix I - Information System Controls Audit Planning Checklist
Appendix II - Tables for Summarizing Work Performed in Evaluating and Testing General and Business Process Application Controls
Appendix III - Tables for Assessing the Effectiveness of General and Business Process Application Controls
Appendix IV - Mapping of FISCAM to NIST SP 800-53 And Other Related NIST Publications
Clifton Gunderson LLP
Certified Public Accountants & Consultants
Count on Insight™
59


FISCAM Appendices
Appendix V - Knowledge, Skills, and Abilities Needed to Perform Information System Controls Audits
Appendix VI - Scope of an Information System Controls Audit in Support of a Financial Audit
Appendix VII - Entity's Use of Service Organizations
Appendix VIII - Application of FISCAM to Single Audits
Appendix IX - Application of FISCAM to FISMA
Appendix X - Information System Controls Audit Documentation
Clifton Gunderson LLP
Certified Public Accountants & Consultants
Count on Insight™
60

Penetration Testing

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

Clifton Gunderson LLP
Certified Public Accountants & Consultants

Count on Insight™

61

GAO Position

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

Clifton Gunderson LLP
Certified Public Accountants & Consultants

Count on Insight™

62

Tools and Techniques

Internet Available Tools and Information

- Freeware
- Shareware
- Commercial Software

Clifton Gunderson LLP
Certified Public Accountants & Consultants

Count on Insight™

63

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

Clifton Gunderson LLP
Certified Public Accountants & Consultants

Count on Insight™

64

Common Vulnerabilities

- 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

Clifton Gunderson LLP
Certified Public Accountants & Consultants

Count on Insight™

65

Questions?

Ronald E. Franke, CISA, CIA, CFE, CICA

Ron.Franke@cliftoncpa.com

(512) 342-0800

Clifton Gunderson LLP
Certified Public Accountants & Consultants

Count on Insight™

66