


CAPLAW
Community Action Program Legal Services, Inc.

*Keys to Cost Effective Controls & Clean Audits:
The COSO Internal Control
Integrated Framework*

*July 27, 2011
Presented by Kay Sohl*

Part of the Beyond The Basics webinar series



© 2011 Community Action Program Legal Services, Inc.

Webinar Goals:

- Use **COSO framework** to **streamline** and **improve** controls and compliance
- Identify and address **potential audit findings**
- **Reduce** audit time and **cost**

CAPLAW 2

Topics:

- What is **COSO**
- **Why does it matter** to CAAs
- Documenting your system of controls
- **Top control risks** for CAAs
- **Streamlining** controls
- **Next steps**

CAPLAW 3

COSO Basics:

- **C**ommittee of **S**ponsoring **O**rganizations (**COSO**)
- Formed in 1985 to sponsor National Commission on Fraudulent Financial Reporting
- Sponsored jointly by: AAA, AICPA, FEI, IIA, and IMA

CAPLAW

4

COSO Internal Control Publications

- 1992 Internal Control – **I**ntegrated **F**ramework
- 2006 – Internal Control for Financial Reporting
- 2009 – Guidance for Monitoring Internal Control
- 2010 – project to update 1992 framework

CAPLAW

5

Auditors Use COSO Framework to:

- Understand **e**nvironment
- Identify and evaluate **r**isks
- Understand **c**ontrols & evaluate adequacy
- Design **t**ests of controls
- Identify **f**indings

CAPLAW

6

CAAs Use COSO Framework

- Develop **cost effective approach** to controls
- Identify & address **risk**
- **Document** system of controls
- **Reduce** audit cost
- **Avoid** audit findings

CAPLAW

7

COSO Internal Control Framework



CAPLAW

8

Framework: 5 Key Elements

- Control Environment
- Risk Assessment
- Control Activities
- Information & Communication
- Monitoring

CAPLAW

9

Apply COSO Framework for Internal Controls to:

- Operations
- Financial Reporting
- Compliance

CAPLAW

10

Apply COSO Framework to:

- Each program
- Management
- Fund raising
- All activities

CAPLAW

11

Bottom Line Reality:

- CAA use of COSO framework can reduce audit cost and risk of findings
- COSO framework can increase cost effectiveness of controls
- COSO framework can reduce risk of fraud and non-compliance

CAPLAW

12

COSO defines Internal Control

A process effected by an entity's board of directors, management & other personnel, designed to provide reasonable assurance regarding achievement of objectives in...

- Effectiveness & efficiency in operations
- Reliability of financial reporting
- Compliance with applicable laws & regulations

Internal Controls designed to:

- Reduce the risk of improper actions
- Increase the likelihood that errors or wrong acts will be detected
- Reduce the risk that error will go uncorrected

Controls Designed to Prevent

- Misstatement:
 - Financial statements do not fairly present financial condition
- Misappropriation:
 - Theft or misuse of the organization's assets
- Non-Compliance:

Reality

- No perfect controls
- Controls provide **reasonable assurance**, not absolute assurance
- **Cost/benefit analysis** essential in designing, implementing, & monitoring controls

CAPLAW

16

Core Control Concepts

- Internal control is not one event, but a **series of actions** and **activities** that occur throughout an entity's operation on an ongoing basis
- **Integral part** of each **system** used to regulate & guide operations
- **Control environment** is foundation for effective controls

CAPLAW

17

Comprehensive Controls

- Highest levels of **management & governance**
- **Compliance** with law/regulation
- **Program** activities
- Operational **policies & procedures**
- Internal & external **reporting**

CAPLAW

18

COSO Framework

1. Control environment
2. Risk assessment
3. Control activities
4. Information & effective communication
5. Monitoring

**Control Environment:
Board oversight of controls**

- Annual audit
- Audit committee /auditor communication
- CEO annual review
- Follow-up on audit/monitoring findings
- Review of monthly financial statements
- Awareness of most significant risks

**Control Environment:
CEO & Management**

- CEO/Management awareness of high risk areas
- Adequacy of resources for fiscal and program management
- Monthly analysis of financial statements
- Authority/responsibility for compliance clearly assigned

Pre-Call Survey

When does your top management team discuss your control environment?

- Never – 6%
- Monthly/ongoing – 11%
- Internal reports of problems – 17%
- When auditors raise concerns – 33%
- Part of annual goal setting – 39%

CAPLAW

22

**Risk Assessment:
Risk Factors**

- Materiality of exposure – \$\$\$ at risk
- Complexity of compliance requirements
- Experience/lack of experience with program
- Weak control environment/lack of management expertise

CAPLAW

23

**Risk Assessment:
More Risk Factors**

- Financial pressure
- Failure to address previous findings
- Change in CFO

CAPLAW

24

Control Activities:
High Level Controls:

- Top level review of accomplishments
- Comparison of actual to planned, both \$\$\$ & activities
- HR management to employ competent, high integrity staff
- Info processing controls

CAPLAW

25

Control Activities:
Operational Controls

- Physical control of assets
- Segregation of duties
- Proper execution of transactions
- Accurate/timely recording
- Access restrictions & accountability
- Documentation of transactions & controls

CAPLAW

26

Control Activities:
Compliance Controls

- Identification of compliance requirements
- Personal activity reporting to substantiate personnel related charges
- Sub-recipient monitoring
- Procurement
- Cash Management

CAPLAW

27

Control Activities:
Key Compliance Controls *(continued)*

- Allowable costs – including allocated costs
- Facilities & equipment controls

CAPLAW

28

COSO Framework

1. Control environment
2. Risk assessment
3. Control activities
4. Information & effective communication
5. Monitoring

CAPLAW

29

Info & Communications:
Key Elements

- Expectations, policies, procedures communicated clearly throughout organization
- Relevant, reliable, & timely access to programmatic & financial info for managers???

CAPLAW

30

**Monitoring:
Identifying Control Breakdowns**

- Is responsibility for periodic testing of compliance clearly assigned & adequate time available for timely testing?
- Responsibility for follow-up on prior findings clearly assigned with realistic timeline for resolution?

CAPLAW

31

Pre-Call Survey

Status of your written Fiscal Policies and Procedures?

- Complete, clear, updated – 33%
- Reasonably complete – 44%
- Mixed – 22%

CAPLAW

32

Auditors & COSO

- Standards for independent audits require evaluation of internal controls
- A-133 requires additional consideration of controls to ensure compliance
- Increasing emphasis on auditor understanding of risks specific to each organization

CAPLAW

33

Auditing Standards Require Auditor to:

- Understand the nature of the “business”
- Assess risks of misstatement & noncompliance
- Understand controls to address risks
- Test controls
- Analyze results of test
- Determine significance of problems

More Auditor Analysis

- Are controls **working as designed**?
- How **likely** is it that the controls have failed
 - To deter and or detect error or improper action
 - To result in correction of error
- How **significant** would be the consequences be if the controls failed?

Internal Control Findings

- Material Weakness
- Significant Deficiency

A-133 Requires Auditor to:

- Determine whether organization is a **high or low risk auditee**
- Determine whether the organization has received awards through federal **programs** that are **deemed high risk**
- **Tailor audit procedures** & tests to address the level of risk

CAPLAW

37

Auditor must plan A-133 audit to obtain “low” control risk

- **“Low” control risk requires:**
 - Reliable controls
 - Controls operate effectively
- **Auditor gets to “low” control risk by:**
 - Documenting understanding of controls
 - Testing control design and implementation
 - Testing control effectiveness

CAPLAW

38

Compliance Testing

- If controls are found to be effective, auditor uses similar sized samples sizes to test compliance
- If controls are found to be not effective, **sample sizes need to be significantly increased** to determine compliance

CAPLAW

39

Audit Costs

- Time = \$\$\$\$
- Reduce audit time by documenting:
 - Control systems
 - Risk assessment process & results
 - Training & monitoring systems
 - Compliance requirements
 - System changes

CAPLAW

40

Pre-Call Survey

Has your auditor discussed the COSO framework with your CAA?

- Yes – 6%
- No – 61%
- Unsure – 33%

CAPLAW

41

Steps to Reduce Likelihood of Findings

- Improve control environment
- Identify compliance requirements
- Streamline controls
- Improve internal communication
- Internal testing of financial & program compliance

CAPLAW

42

Top CAA Control Risks

- Compliance breakdown
 - Failure to identify & communicate compliance requirements
 - Training & supervision glitches
 - Lack of time for review & testing of financial & program data
 - Cost allocation implementation problems

CAPLAW

43

More CAA Control Risks:

- Inadequate or outdated documentation of control systems, policies, procedures
- Control of assets purchased with federal \$\$\$:
 - Equipment
 - Inventory

CAPLAW

44

Fraud Risks:

- Phantom employee or vendor
- Payroll & benefits manipulation
- Expense reimbursement
- Misuse of CAA credit cards or accounts
- Misuse of equipment
- Corruption, exchange of favors

CAPLAW

45

Rethinking Controls

- Document Major Processes
 - Revenue & expense cycles
 - Payroll cycle
 - Contract management cycle
 - GL closing & reporting cycle
 - Budget cycle

Tools for Documentation

- Flow charts
- Process level matrix
- Narratives

Identify Purpose of Control Procedures

- Prevent error
- Detect error
- Establish accountability
- Deter fraud
- Document compliance

Opportunities to Streamline Controls

- Eliminate **duplicative** controls
 - Multiple steps designed to achieve same purpose
- Complete or eliminate **incomplete** controls
 - Records maintained for comparison, but no comparison made
 - Authorization required but not reviewed

Common Ineffective Controls

- **Check-logs** never compared to GL or bank records
- **Purchase Orders** not systematically recorded, matched, investigated
- **Un-reconciled systems** for tracking accrual and use of sick & vacation time
- Check signature requirements

Opportunities for Streamlining

- Remote deposit
- Outsourced A/P
- Third party benefits administration
- **Cloud applications** for mobile staff data entry
- Generation of accurate supporting records through **improved design of database systems**

COSO Enterprise Risk Management

- 2004 – Enterprise Risk Management- Integrated Framework
- ERM broadens framework for Internal Controls to include highest level evaluation of organization-wide risks
- Involves setting strategy & identifying specific potential events, and defining risk appetite

CAPLAW

52

Pre-Call Survey

Has your CAA explicitly assigned responsibility for ERM- Entity-Wide Risk Management ?

- Yes – 35%
- No – 47%
- Unsure – 18%

CAPLAW

53

Your Next Steps?

- Use COSO framework to analyze your internal controls
- Flowchart controls
- Identify weak or missing controls
- Eliminate unproductive controls
- Improve communications & monitoring
- Increase focus on Enterprise Risk Management

CAPLAW

54

Resources

- Download a free executive summary of the COSO report on Internal Control Integrated Framework
<http://www.coso.org/IC-IntegratedFramework-summary.htm>

Control Review Checklist

Control	Control documentation reviewed	Reviewed by	Review date
Control Environment			
Conflict of Interest P&P			
Whistleblower Policy			
Code of Ethics/Integrity policy			
Board evaluation of CEO			
Board review of compensation & management capacity			
Board review of monthly financial statements			
Board audit committee/auditor discussions			
Board review of resolution of audit & monitoring findings			
Board review of programmatic accomplishments			
Other			
General Risk Assessment			
External risk review including funding environment, community perception, changing demand/need for services			
Review and update of internal risk identification			
Exposure analysis- ranking of risks by significance of potential losses and likelihood of occurrence			
Contract Compliance Risk Assessment:			
OMB A-110 requirements			
• Allowable activities			
• Allowable cost			
• Cash management			
• Davis Bacon act			
• Eligibility			
• Equip/Real Property management			
• Matching/level of effort			
• Period of availability of fed funds			
• Procurement, suspension & debarment			
• Program income			
• Real property acquisition			
• Reporting			
• Sub recipient monitoring			
• Special tests & provisions			
OMB A-122 requirements			
• Current approved federal indirect cost rate			
• Written cost allocation plan			
• Monitoring of actual indirect costs in comparison to budget			

Control Review Checklist

Control	Control documentation reviewed	Reviewed by	Review date
CFR Requirements			
<ul style="list-style-type: none"> • Review of CFRs for each funding source • Policies & procedures to assure compliance with CFR requirements varying from OMB Circulars 			
Control Activities			
Written fiscal and operational policies & procedures			
Top management review of financial & program activities			
Management reviews at program or functional level			
Controls over info processing/IT			
Physical controls over vulnerable assets			
Review of performance indicators			
Segregation of duties			
Proper execution of transactions & events			
Accurate & timely recording of events			
Access restrictions & accountability for resources & records			
Appropriate documentation of transactions & internal control			
Information & Communication			
Monthly financial reporting at program and organization level			
Monthly program accomplishment reporting at program & organizational level			
Manager access to operational and financial data as needed for planning and oversight			
Structures, policies, and procedures to encourage open information flow among all levels of the organization			
Monitoring			
Monthly comparison of planned program and financial activity to actual reviewed by program managers, top management, & Board			
System for tracking all audit & monitoring findings and their correction or resolution			
Responsibility for achieving correction or resolution of all findings clearly assigned			
Authority to resolve/correct findings clearly assigned			

Control Review Checklist

Control	Control documentation reviewed	Reviewed by	Review date
Monitoring – continued			
Progress resolving/correcting findings monitored regularly by CEO & Board			
Reconciliations to verify financial & program data reports routinely completed and reviewed by managers			

November 1999

Standards for Internal Control in the Federal Government



G A O

Accountability * Integrity * Reliability

Foreword

Federal policymakers and program managers are continually seeking ways to better achieve agencies' missions and program results, in other words, they are seeking ways to improve accountability. A key factor in helping achieve such outcomes and minimize operational problems is to implement appropriate internal control. Effective internal control also helps in managing change to cope with shifting environments and evolving demands and priorities. As programs change and as agencies strive to improve operational processes and implement new technological developments, management must continually assess and evaluate its internal control to assure that the control activities being used are effective and updated when necessary.

The Federal Managers' Financial Integrity Act of 1982 (FMFIA) requires the General Accounting Office (GAO) to issue standards for internal control in government. The standards provide the overall framework for establishing and maintaining internal control and for identifying and addressing major performance and management challenges and areas at greatest risk of fraud, waste, abuse, and mismanagement. Office of Management and Budget (OMB) Circular A-123, Management Accountability and Control, revised June 21, 1995, provides the specific requirements for assessing and reporting on controls. The term internal control in this document is synonymous with the term management control (as used in OMB Circular A-123) that covers all aspects of an agency's operations (programmatic, financial, and compliance).

Recently, other laws have prompted renewed focus on internal control. The Government Performance and Results Act of 1993 requires agencies to clarify their missions, set strategic and annual performance goals, and measure and report on performance

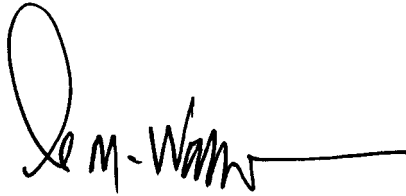
toward those goals. Internal control plays a significant role in helping managers achieve those goals. Also, the Chief Financial Officers Act of 1990 calls for financial management systems to comply with internal control standards, and the Federal Financial Management Improvement Act of 1996 identifies internal control as an integral part of improving financial management systems.

Rapid advances in information technology have highlighted the need for updated internal control guidance related to modern computer systems. The management of human capital has gained recognition as a significant part of internal control. Furthermore, the private sector has updated its internal control guidance with the issuance of Internal Control — Integrated Framework, published by the Committee of Sponsoring Organizations of the Treadway Commission (COSO). Consequently, we have developed this standards update which supersedes our previously issued “Standards for Internal Controls in the Federal Government.”

This update gives greater recognition to the increasing use of information technology to carry out critical government operations, recognizes the importance of human capital, and incorporates, as appropriate, the relevant updated internal control guidance developed in the private sector. The standards are effective beginning with fiscal year 2000 and the Federal Managers Financial Integrity Act reports covering that year.

Foreword

We appreciate the efforts of government officials, public accounting professionals, and other members of the financial community and academia who provided valuable assistance in developing these standards.

A handwritten signature in black ink, appearing to read "D. M. Walker", with a long horizontal line extending to the right.

David M. Walker
Comptroller General
of the United States

Introduction

The following definition, objectives, and fundamental concepts provide the foundation for the internal control standards.

Definition and Objectives

Internal Control

An integral component of an organization's management that provides reasonable assurance that the following objectives are being achieved:

- effectiveness and efficiency of operations,
- reliability of financial reporting, and
- compliance with applicable laws and regulations.

Internal control is a major part of managing an organization. It comprises the plans, methods, and procedures used to meet missions, goals, and objectives and, in doing so, supports performance-based management. Internal control also serves as the first line of defense in safeguarding assets and preventing and detecting errors and fraud. In short, internal control, which is synonymous with management control, helps government program managers achieve desired results through effective stewardship of public resources.

Internal control should provide reasonable assurance that the objectives of the agency are being achieved in the following categories:

Introduction

- Effectiveness and efficiency of operations including the use of the entity's resources.
- Reliability of financial reporting, including reports on budget execution, financial statements, and other reports for internal and external use.
- Compliance with applicable laws and regulations.

A subset of these objectives is the safeguarding of assets. Internal control should be designed to provide reasonable assurance regarding prevention of or prompt detection of unauthorized acquisition, use, or disposition of an agency's assets.

Fundamental Concepts

Internal Control

- A continuous built-in component of operations.
- Effected by people.
- Provides reasonable assurance, not absolute assurance.

The fundamental concepts provide the underlying framework for designing and applying the standards.

Internal Control Is a Continuous Built-in Component of Operations

Internal control is not one event, but a series of actions and activities that occur throughout an entity's operations and on an ongoing basis. Internal control should be recognized as an integral part of each system that management uses to regulate and guide its operations rather than as a separate system within an agency. In this sense, internal control is management control that is built into the entity as a

Introduction

part of its infrastructure to help managers run the entity and achieve their aims on an ongoing basis.

Internal Control Is Effected by People

People are what make internal control work. The responsibility for good internal control rests with all managers. Management sets the objectives, puts the control mechanisms and activities in place, and monitors and evaluates the control. However, all personnel in the organization play important roles in making it happen.

Internal Control Provides Reasonable Assurance, Not Absolute Assurance

Management should design and implement internal control based on the related cost and benefits. No matter how well designed and operated, internal control cannot provide absolute assurance that all agency objectives will be met. Factors outside the control or influence of management can affect the entity's ability to achieve all of its goals. For example, human mistakes, judgment errors, and acts of collusion to circumvent control can affect meeting agency objectives. Therefore, once in place, internal control provides reasonable, not absolute, assurance of meeting agency objectives.

Internal Control Standards

Presentation of the Standards

The Five Standards for Internal Control

- Control Environment
- Risk Assessment
- Control Activities
- Information and Communications
- Monitoring

These standards define the minimum level of quality acceptable for internal control in government and provide the basis against which internal control is to be evaluated. These standards apply to all aspects of an agency's operations: programmatic, financial, and compliance. However, they are not intended to limit or interfere with duly granted authority related to developing legislation, rule-making, or other discretionary policy-making in an agency. These standards provide a general framework. In implementing these standards, management is responsible for developing the detailed policies, procedures, and practices to fit their agency's operations and to ensure that they are built into and an integral part of operations.

In the following material, each of these standards is presented in a short, concise statement. Additional information is provided to help managers incorporate the standards into their daily operations.

Control Environment

Management and employees should establish and maintain an environment throughout the organization that sets a positive and supportive attitude toward internal control and conscientious management.

A positive control environment is the foundation for all other standards. It provides discipline and structure as well as the climate which influences the quality of internal control. Several key factors affect the control environment.

One factor is the integrity and ethical values maintained and demonstrated by management and staff. Agency management plays a key role in providing leadership in this area, especially in setting and maintaining the organization's ethical tone, providing guidance for proper behavior, removing temptations for unethical behavior, and providing discipline when appropriate.

Another factor is management's commitment to competence. All personnel need to possess and maintain a level of competence that allows them to accomplish their assigned duties, as well as understand the importance of developing and implementing good internal control. Management needs to identify appropriate knowledge and skills needed for various jobs and provide needed training, as well as candid and constructive counseling, and performance appraisals.

Management's philosophy and operating style also affect the environment. This factor determines the degree of risk the agency is willing to take and management's philosophy towards performance-based management. Further, the attitude and philosophy of management toward information systems, accounting, personnel functions, monitoring, and audits and evaluations can have a profound effect on internal control.

Another factor affecting the environment is the agency's organizational structure. It provides management's framework for planning, directing, and controlling operations to achieve agency objectives. A good internal control environment requires that the agency's organizational structure clearly define key areas of authority and responsibility and establish appropriate lines of reporting.

The environment is also affected by the manner in which the agency delegates authority and responsibility throughout the organization. This delegation covers authority and responsibility for operating activities, reporting relationships, and authorization protocols.

Good human capital policies and practices are another critical environmental factor. This includes establishing appropriate practices for hiring, orienting, training, evaluating, counseling, promoting, compensating, and disciplining personnel. It also includes providing a proper amount of supervision.

A final factor affecting the environment is the agency's relationship with the Congress and central oversight agencies such as OMB. Congress mandates the programs that agencies undertake and monitors their progress and central agencies provide policy and guidance on many different matters. In addition,

Inspectors General and internal senior management councils can contribute to a good overall control environment.

Risk Assessment

Internal control should provide for an assessment of the risks the agency faces from both external and internal sources.

A precondition to risk assessment is the establishment of clear, consistent agency objectives. Risk assessment is the identification and analysis of relevant risks associated with achieving the objectives, such as those defined in strategic and annual performance plans developed under the Government Performance and Results Act, and forming a basis for determining how risks should be managed.

Management needs to comprehensively identify risks and should consider all significant interactions between the entity and other parties as well as internal factors at both the entitywide and activity level. Risk identification methods may include qualitative and quantitative ranking activities, management conferences, forecasting and strategic planning, and consideration of findings from audits and other assessments.

Once risks have been identified, they should be analyzed for their possible effect. Risk analysis generally includes estimating the risk's significance, assessing the likelihood of its occurrence, and

deciding how to manage the risk and what actions should be taken. The specific risk analysis methodology used can vary by agency because of differences in agencies' missions and the difficulty in qualitatively and quantitatively assigning risk levels.

Because governmental, economic, industry, regulatory, and operating conditions continually change, mechanisms should be provided to identify and deal with any special risks prompted by such changes.

Control Activities

Internal control activities help ensure that management's directives are carried out. The control activities should be effective and efficient in accomplishing the agency's control objectives.

Control activities are the policies, procedures, techniques, and mechanisms that enforce management's directives, such as the process of adhering to requirements for budget development and execution. They help ensure that actions are taken to address risks. Control activities are an integral part of an entity's planning, implementing, reviewing, and accountability for stewardship of government resources and achieving effective results.

Control activities occur at all levels and functions of the entity. They include a wide range of diverse activities such as approvals, authorizations, verifications, reconciliations, performance reviews,

maintenance of security, and the creation and maintenance of related records which provide evidence of execution of these activities as well as appropriate documentation. Control activities may be applied in a computerized information system environment or through manual processes.

Activities may be classified by specific control objectives, such as ensuring completeness and accuracy of information processing.

Examples of Control Activities

- Top level reviews of actual performance,
- Reviews by management at the functional or activity level,
- Management of human capital,
- Controls over information processing,
- Physical control over vulnerable assets,
- Establishment and review of performance measures and indicators,
- Segregation of duties,
- Proper execution of transactions and events,
- Accurate and timely recording of transactions and events,
- Access restrictions to and accountability for resources and records, and
- Appropriate documentation of transactions and internal control.

There are certain categories of control activities that are common to all agencies. Examples include the following:

Internal Control Standards

Top Level Reviews of Actual Performance	Management should track major agency achievements and compare these to the plans, goals, and objectives established under the Government Performance and Results Act.
Reviews by Management at the Functional or Activity Level	Managers also need to compare actual performance to planned or expected results throughout the organization and analyze significant differences.
Management of Human Capital	Effective management of an organization's workforce—its human capital—is essential to achieving results and an important part of internal control. Management should view human capital as an asset rather than a cost. Only when the right personnel for the job are on board and are provided the right training, tools, structure, incentives, and responsibilities is operational success possible. Management should ensure that skill needs are continually assessed and that the organization is able to obtain a workforce that has the required skills that match those necessary to achieve organizational goals. Training should be aimed at developing and retaining employee skill levels to meet changing organizational needs. Qualified and continuous supervision should be provided to ensure that internal control objectives are achieved. Performance evaluation and feedback, supplemented by an effective reward system, should be designed to help employees understand the connection between their performance and the organization's success. As a part of its human capital planning, management should also consider how best to retain valuable employees, plan for their eventual succession, and ensure continuity of needed skills and abilities.
Controls Over Information Processing	A variety of control activities are used in information processing. Examples include edit checks of data entered, accounting for transactions in numerical sequences, comparing file totals with control

Internal Control Standards

accounts, and controlling access to data, files, and programs. Further guidance on control activities for information processing is provided below under “Control Activities Specific for Information Systems.”

Physical Control Over Vulnerable Assets

An agency must establish physical control to secure and safeguard vulnerable assets. Examples include security for and limited access to assets such as cash, securities, inventories, and equipment which might be vulnerable to risk of loss or unauthorized use. Such assets should be periodically counted and compared to control records.

Establishment and Review of Performance Measures and Indicators

Activities need to be established to monitor performance measures and indicators. These controls could call for comparisons and assessments relating different sets of data to one another so that analyses of the relationships can be made and appropriate actions taken. Controls should also be aimed at validating the propriety and integrity of both organizational and individual performance measures and indicators.

Segregation of Duties

Key duties and responsibilities need to be divided or segregated among different people to reduce the risk of error or fraud. This should include separating the responsibilities for authorizing transactions, processing and recording them, reviewing the transactions, and handling any related assets. No one individual should control all key aspects of a transaction or event.

Proper Execution of Transactions and Events

Transactions and other significant events should be authorized and executed only by persons acting within the scope of their authority. This is the principal means of assuring that only valid transactions to exchange, transfer, use, or commit resources and other events are initiated or entered

Internal Control Standards

into. Authorizations should be clearly communicated to managers and employees.

Accurate and Timely
Recording of
Transactions and Events

Transactions should be promptly recorded to maintain their relevance and value to management in controlling operations and making decisions. This applies to the entire process or life cycle of a transaction or event from the initiation and authorization through its final classification in summary records. In addition, control activities help to ensure that all transactions are completely and accurately recorded.

Access Restrictions to
and Accountability for
Resources and Records

Access to resources and records should be limited to authorized individuals, and accountability for their custody and use should be assigned and maintained. Periodic comparison of resources with the recorded accountability should be made to help reduce the risk of errors, fraud, misuse, or unauthorized alteration.

Appropriate
Documentation of
Transactions and
Internal Control

Internal control and all transactions and other significant events need to be clearly documented, and the documentation should be readily available for examination. The documentation should appear in management directives, administrative policies, or operating manuals and may be in paper or electronic form. All documentation and records should be properly managed and maintained.

These examples are meant only to illustrate the range and variety of control activities that may be useful to agency managers. They are not all-inclusive and may not include particular control activities that an agency may need.

Furthermore, an agency's internal control should be flexible to allow agencies to tailor control activities to fit their special needs. The specific control activities used by a given agency may be different from those

used by others due to a number of factors. These could include specific threats they face and risks they incur; differences in objectives; managerial judgment; size and complexity of the organization; operational environment; sensitivity and value of data; and requirements for system reliability, availability, and performance.

**Control Activities
Specific for
Information Systems**

- General Control
- Application Control

There are two broad groupings of information systems control - general control and application control. General control applies to all information systems—mainframe, minicomputer, network, and end-user environments. Application control is designed to cover the processing of data within the application software.

General Control

This category includes entitywide security program planning, management, control over data center operations, system software acquisition and maintenance, access security, and application system development and maintenance. More specifically:

- Data center and client-server operations controls include backup and recovery procedures, and contingency and disaster planning. In addition, data center operations controls also include job set-up and scheduling procedures and controls over operator activities.

- System software control includes control over the acquisition, implementation, and maintenance of all system software including the operating system, data-based management systems, telecommunications, security software, and utility programs.
- Access security control protects the systems and network from inappropriate access and unauthorized use by hackers and other trespassers or inappropriate use by agency personnel. Specific control activities include frequent changes of dial-up numbers; use of dial-back access; restrictions on users to allow access only to system functions that they need; software and hardware “firewalls” to restrict access to assets, computers, and networks by external persons; and frequent changes of passwords and deactivation of former employees’ passwords.
- Application system development and maintenance control provides the structure for safely developing new systems and modifying existing systems. Included are documentation requirements; authorizations for undertaking projects; and reviews, testing, and approvals of development and modification activities before placing systems into operation. An alternative to in-house development is the procurement of commercial software, but control is necessary to ensure that selected software meets the user’s needs, and that it is properly placed into operation.

Application Control

This category of control is designed to help ensure completeness, accuracy, authorization, and validity of all transactions during application processing. Control should be installed at an application’s interfaces with other systems to ensure that all inputs are received and are valid and outputs are correct and properly distributed. An example is computerized edit checks built into the system to review the format, existence, and reasonableness of data.

General and application control over computer systems are interrelated. General control supports the functioning of application control, and both are needed to ensure complete and accurate information processing. If the general control is inadequate, the application control is unlikely to function properly and could be overridden.

Because information technology changes rapidly, controls must evolve to remain effective. Changes in technology and its application to electronic commerce and expanding Internet applications will change the specific control activities that may be employed and how they are implemented, but the basic requirements of control will not have changed. As more powerful computers place more responsibility for data processing in the hands of the end users, the needed controls should be identified and implemented.

Information and Communications

Information should be recorded and communicated to management and others within the entity who need it and in a form and within a time frame that enables them to carry out their internal control and other responsibilities.

For an entity to run and control its operations, it must have relevant, reliable, and timely communications relating to internal as well as external events. Information is needed throughout the agency to achieve all of its objectives.

Program managers need both operational and financial data to determine whether they are meeting their agencies' strategic and annual performance plans and meeting their goals for accountability for effective and efficient use of resources. For example, operating information is required for development of financial reports. This covers a broad range of data from purchases, subsidies, and other transactions to data on fixed assets, inventories, and receivables. Operating information is also needed to determine whether the agency is achieving its compliance requirements under various laws and regulations. Financial information is needed for both external and internal uses. It is required to develop financial statements for periodic external reporting, and, on a day-to-day basis, to make operating decisions, monitor performance, and allocate resources. Pertinent information should be identified, captured, and distributed in a form and time frame that permits people to perform their duties efficiently.

Effective communications should occur in a broad sense with information flowing down, across, and up the organization. In addition to internal communications, management should ensure there are adequate means of communicating with, and obtaining information from, external stakeholders that may have a significant impact on the agency achieving its goals. Moreover, effective information technology management is critical to achieving useful, reliable, and continuous recording and communication of information.

Monitoring

Internal control monitoring should assess the quality of performance over time and ensure that the findings of audits and other reviews are promptly resolved.

Internal control should generally be designed to assure that ongoing monitoring occurs in the course of normal operations. It is performed continually and is ingrained in the agency's operations. It includes regular management and supervisory activities, comparisons, reconciliations, and other actions people take in performing their duties.

Separate evaluations of control can also be useful by focusing directly on the controls' effectiveness at a specific time. The scope and frequency of separate evaluations should depend primarily on the assessment of risks and the effectiveness of ongoing monitoring procedures. Separate evaluations may take the form of self-assessments as well as review of control design and direct testing of internal control. Separate evaluations also may be performed by the agency Inspector General or an external auditor. Deficiencies found during ongoing monitoring or through separate evaluations should be communicated to the individual responsible for the function and also to at least one level of management above that individual. Serious matters should be reported to top management.

Monitoring of internal control should include policies and procedures for ensuring that the findings of audits and other reviews are promptly resolved. Managers are to (1) promptly evaluate findings from

audits and other reviews, including those showing deficiencies and recommendations reported by auditors and others who evaluate agencies' operations, (2) determine proper actions in response to findings and recommendations from audits and reviews, and (3) complete, within established time frames, all actions that correct or otherwise resolve the matters brought to management's attention. The resolution process begins when audit or other review results are reported to management, and is completed only after action has been taken that (1) corrects identified deficiencies, (2) produces improvements, or (3) demonstrates the findings and recommendations do not warrant management action.

Ordering Information

The first copy of each GAO report and testimony is free. Additional copies are \$2 each. Orders should be sent to the following address, accompanied by a check or money order made out to the Superintendent of Documents, when necessary. VISA and MasterCard credit cards are accepted, also. Orders for 100 or more copies to be mailed to a single address are discounted 25 percent.

Orders by mail:

**U.S. General Accounting Office
P.O. Box 37050
Washington, DC 20013**

or visit:

**Room 1100
700 4th St. NW (corner of 4th & G Sts. NW)
U.S. General Accounting Office
Washington, DC**

**Orders may also be placed by calling
(202) 512-6000 or by using fax number
(202) 512-6061, or TDD (202) 512-2537.**

Each day, GAO issues a list of newly available reports and testimony. To receive facsimile copies of the daily list or any list from the past 30 days, please call (202) 512-6000 using a touchtone phone. A recorded menu will provide information on how to obtain these lists.

For information on how to access GAO reports on the INTERNET, send an e-mail message with "info" in the body to: info@www.gao.gov

**or visit GAO's World Wide Web Home Page at:
<http://www.gao.gov>**

**United States
General Accounting Office
Washington, D.C. 20548-0001**

**Official Business
Penalty for Private Use \$300**

Address Correction Requested

<p>Bulk Rate Postage & Fees Paid GAO Permit No. G100</p>
