

Internal Controls That Work

Internal Controls That Work: A Practical Guide for Local Governments

Lorrie A Brinson, CPA, CGFO, MBA/PA



#SOGF2026

TOPICS

- The Foundation
- Internal Controls of Daily Transactions
 - Segregation of Duties
- Internal Controls over Financial Reporting & the ACFR
- Internal Controls in the Budget Process
- Internal Controls for Audit Preparation
- Information Technology & System Access Controls
- COSO ERM
- ERM Components
- Internal Control Risk Case Studies
- Q&A
- References



#SOGF2026

COSO stands for the **Committee of Sponsoring Organizations of the Treadway Commission**

It was created as a **private-sector initiative** sponsored by five major professional organizations:

- American Accounting Association (AAA)
- American Institute of Certified Public Accountants (AICPA)
- Financial Executives International (FEI)
- Institute of Management Accountants (IMA)
- The Institute of Internal Auditors (IIA)

COSO develops frameworks and guidance on internal control, enterprise risk management, and fraud deterrence to strengthen organizational performance, oversight, and accountability.



#SOGF2026

The Foundation

Internal control is an ongoing process, carried out by the governing body, management, and employees, that provides reasonable assurance the organization will achieve its operations, reporting, and compliance objectives.

Five COSO Components

Control Environment

Risk Assessment

Control Activities

Information & Communication

Monitoring Activities

Operations • Reporting • Compliance



Control Environment

Definition

The control environment is the foundation for internal control across the organization. It is created by the **standards, processes, structures, and expectations established** by the governing body and management, including the organization's **tone at the top**.

Key elements

- Integrity and ethical values
- Governance oversight, organizational structure, and assignment of authority
- Competence, accountability, and performance expectations



Risk Assessment

Definition

Risk assessment is the **ongoing process** of **identifying and evaluating** internal and external risks that could prevent the organization from achieving its objectives. Those risks are considered in relation to established objectives and risk tolerances so management can determine how they should be addressed.

Key elements

- Clearly defined operations, reporting, and compliance objectives
- Identification and analysis of risks that could affect those objectives
- Consideration of fraud risk and changes that could make controls ineffective



Control Activities

Definition

Control activities are the actions established through policies and procedures to help ensure that management's directives are carried out and risks are reduced to acceptable levels. These activities may be **preventive or detective** and may be **manual or automated**.

Key elements

- Approvals, authorizations, verifications, and reconciliations
- Business performance reviews and technology-related controls
- Segregation of duties or alternative controls when segregation is not practical



#SOGF2026

School of Government | Internal Controls in Local Government

Information and Communication

Definition

Information and communication ensure that **relevant, quality** information is obtained, generated, shared, and used so people can carry out their internal control responsibilities. Communication should flow throughout the organization and also support appropriate communication with external parties.

Key elements

- Reliable information from internal and external sources
- Clear communication of objectives, responsibilities, and expectations
- Information that flows up, down, and across the organization



Monitoring Activities

Definition

Monitoring activities are **ongoing** and/or **separate evaluations** used to determine whether the five components of internal control are **present and functioning**. Identified deficiencies are **evaluated and communicated** to those responsible for corrective action.

Key elements

- Ongoing evaluations built into normal business processes
- Periodic separate evaluations based on risk and management judgment
- Timely communication and follow-up on control deficiencies



Internal Controls of Daily Transactions

Control Environment

Control Activities

Segregation of duties is an internal control principle that divides key responsibilities for a transaction or process among different individuals so that no one person has complete control from beginning to end.

In practice, the main duties that should be separated are **authorization, custody of assets, recordkeeping, and reconciliation/review**. For example, the person who approves a payment ideally should not also prepare the payment, record it in the accounting system, and reconcile the bank account.

Segregation of duties supports internal controls by reducing the risk that errors, fraud, or unauthorized transactions will occur and go undetected. It creates natural checks and balances within a process because one employee's work is reviewed, verified, or completed by another.

****Compensating controls can be used in smaller local governments. No one person should be able to initiate, approve, record, and reconcile the same transaction.***



#SOGF2026

Internal Controls over Financial Reporting & Annual Comprehensive Financial Report

For **financial reporting**, all five COSO components work together, but the components most directly tied to making sure the organization is achieving its **operations, reporting, and compliance objectives** are **Risk Assessment, Control Activities, and Monitoring Activities**.

Risk Assessment

Risk Assessment helps management identify what could prevent the organization from meeting its financial, operational, budgetary, or compliance goals. For example, a local government may identify risks such as revenue shortfalls, budget overruns, inaccurate financial reporting, or noncompliance with purchasing requirements.



#SOGF2026

Internal Controls over Financial Reporting & Annual Comprehensive Financial Report

Control Environment

Control Environment establishes accountability, ethical expectations, and management oversight.

Control Activities are the actual policies and procedures put in place to address those risks. In the budget and financial reporting process, examples include budget-to-actual reviews, reconciliations, approval requirements, variance analysis, journal entry review, and controls over financial statement preparation.

Control Activities

Information & Communication

Information and Communication ensures that accurate financial and budget information reaches the right people in time to make decisions.

Monitoring Activities provide assurance that those controls are actually working as intended. Management reviews, periodic reconciliations, internal reviews, audit findings, and follow-up on budget variances are all examples of monitoring.

Monitoring Activities

All five COSO components of Internal Controls should be present and working together whether developing management reports or external reports. Monitoring monthly or quarterly tells us whether the controls are actually working.



#SOGF2026

Internal Control over the Budget Process

Monitoring Activities

For the budget process specifically, monitoring is especially important because regular budget-to-actual comparisons help management determine whether the organization is on track to meet its operational and compliance objectives.

Risk Assessment

Risk assessment throughout the process identifies what could keep the organization from meeting their goals. Control activities help prevent or detect those problems; and monitoring tell whether objectives are being met.



#SOGF2026

Internal Control over the Audit Preparation

Internal control works best when audit preparation is an ongoing process—not a year-end scramble.

Control Environment

Control Activities

- Maintain a monthly and year-end closing calendar (checklist) with assigned owners and due dates.
- Complete bank, receivable, payable, payroll, debt, grant, and subsidiary ledger reconciliations on a consistent schedule.
- Require documented review of reconciliations, journal entries, estimates, and year-end adjustments.
- Maintain organized support for balances and transactions so audit evidence is available when requested.

Information & Communication

Monitoring Activities

- Use a centralized Prepared-by-Client (PBC) request tracker and secure document repository.
- Communicate deadlines and responsibilities to finance, payroll, grants, utilities, public works, and other departments.
- Review prior-year audit findings and open corrective actions before the next audit begins.
- Escalate unresolved reconciling items, missing support, or late schedules to management early.



Internal Control Over the Audit Preparation

Risk Assessment

- Identify high-risk areas before year-end: grants, capital assets, debt, leases, pensions/OPEB, payroll accruals, and unusual transactions.
- Consider changes in staffing, systems, accounting standards, contracts, or funding sources that could affect reporting.
- Assess fraud and management-override risks, including unusual journal entries and transactions posted near period-end.
- Prioritize audit-preparation effort based on significance and likelihood of error.

Control Activities

Monitoring Activities

- Perform independent tie-outs of supporting schedules to the general ledger and draft financial statements.
- Resolve old reconciling items and investigate recurring audit adjustments rather than carrying them forward.
- Document the basis for significant estimates and management judgments.
- After the audit, analyze proposed adjustments and findings to determine whether a process, policy, training, or system control should change.



Internal Control Over the IT System Access Control

Access to financial systems should be based on job responsibilities and limited to what each user needs to perform assigned duties.

Govern Access and Define Responsibility

Control Environment

Information & Communication

- Establish written access standards and assign responsibility for approving, provisioning, changing, and removing access.
- Use unique user IDs; avoid shared accounts where individual accountability is needed.
- Define roles for finance, payroll, purchasing, utility billing, cash receipts, and system administration.
- Coordinate HR, department management, IT, and finance so employee status changes trigger timely access changes.

Apply Preventive Access Controls

Control Activities

Risk Assessment

- Grant access using least-privilege and role-based principles; require approval before new or expanded access is assigned.
- Use multifactor authentication where supported, especially for remote or privileged access.
- Separate incompatible functions—for example, vendor setup from payment approval or payroll setup from payroll processing.
- Restrict administrator privileges and document emergency or temporary elevated access.



Internal Control Over the IT System Access Control

Review and Recertify Access

Monitoring Activities

Control Activities

- Perform periodic user-access reviews by system and department; confirm each user still needs assigned roles.
- Review privileged and administrator accounts separately because they present greater risk.
- Disable inactive accounts and remove access promptly for terminated or transferred employees.
- Retain evidence of the review, including exceptions identified, corrections made, and reviewer approval.

Use System Information to Detect Problems

Information & Communication

Risk Assessment

Monitoring Activities

- Review audit logs, failed login activity, role changes, and significant configuration or master-file changes where available.
- Investigate access exceptions and document corrective action.
- Communicate significant access issues to finance leadership, management, and governing oversight when appropriate.
- Reassess access risks when software, staffing, vendors, or business processes change.



What Is COSO Enterprise Risk Management (ERM)?

COSO ERM is...

The culture, capabilities, and practices an organization integrates with strategy-setting and applies while carrying out that strategy to manage risk in creating, preserving, and realizing value.

It is broader than a risk list or a single department. COSO emphasizes that ERM is embedded in decision-making, governance, strategy, performance, and communication.

Why it matters

- Helps management consider risk when selecting and carrying out strategy.
- Supports board oversight of risk appetite, strategy, performance, and significant change.
- Connects risk to performance rather than treating risk as an isolated exercise.
- Applies to organizations of any size, including government agencies.



Governance and Culture

Governance sets the organization's tone and establishes oversight responsibilities for enterprise risk management. Culture reflects the organization's ethical values, desired behaviors, and understanding of risk.

Related ERM principles

- Board risk oversight
- Operating structures
- Desired culture and core values
- Attracting, developing, and retaining capable individuals



Strategy and Objective-Setting

Enterprise risk management, strategy, and objective-setting work together in strategic planning. Risk appetite is aligned with strategy, and business objectives provide the basis for identifying, assessing, and responding to risk.

Related ERM principles

- Analyze the business context
- Define risk appetite
- Evaluate alternative strategies
- Formulate business objectives



Performance

Risks that may affect strategy and business objectives are identified and assessed. Risks are prioritized by severity and risk appetite, appropriate responses are selected, and management considers the portfolio view of risk.

Related ERM principles

- Identify risk
- Assess severity and prioritize risks
- Implement risk responses
- Develop a portfolio view of risk



Review and Revision

By reviewing entity performance, the organization considers how well the ERM components are functioning over time, how substantial changes affect the organization, and what revisions are needed.

Related ERM principles

- Assess substantial change
- Review risk and performance
- Pursue improvement in enterprise risk management



Information, Communication, and Reporting

Enterprise risk management requires a continual process of obtaining and sharing necessary information from internal and external sources, with information flowing up, down, and across the organization.

Related ERM principles

- Leverage information and technology
- Communicate risk information
- Report on risk, culture, and performance



COSO Internal Control vs. COSO ERM

Distinct frameworks with different focuses that are designed to work together

Area	COSO Internal Control	COSO ERM
Primary focus	Reasonable assurance over operations, reporting, and compliance objectives.	Integrating risk with strategy and performance to create, preserve, and realize value.
Orientation	Control design, implementation, operation, and evaluation.	Strategy selection, risk appetite, performance, change, and enterprise-wide risk.
Five components	Control Environment; Risk Assessment; Control Activities; Information C Communication; Monitoring Activities.	Governance C Culture; Strategy C Objective-Setting; Performance; Review C Revision; Information, Communication C Reporting.
How risk is addressed	Risk is assessed so controls can be designed to reduce risk to achievement of objectives.	Risk is considered in strategy, business objectives, performance, and portfolio-level decision-making.
Relationship	Remains the primary COSO framework for internal control.	Addresses more than internal control; the two frameworks are distinct, connected, and neither supersedes the other.



#SOGF202426

KEY TAKEAWAY

COSO Internal Control helps an organization control and monitor its processes; COSO ERM broadens the lens to connect risk directly to strategy, objectives, performance, and value.



#SOGF2026

COSO COMPONENTS APPLIED

COSO Component	Local Government Application
Control Environment	Management establishes purchasing policies and accountability.
Risk Assessment	Management identifies risks such as unauthorized purchases, duplicate payments, or fraud.
Control Activities	Purchase orders, approvals, invoice matching, and segregation of duties address those risks.
Information & Communication	Employees receive purchasing procedures and management receives expenditure reports.
Monitoring Activities	Finance reviews exceptions, budget variances, purchasing activity, and audit findings.



#SOGF2026

Segregation-of-Duties Scenario

Participants identify conflicting duties in a small finance office and recommend compensating controls.

Scenario Background

The Town Clerk is one of only 2 full-time staff in the office. The other full-time staff is a clerk that answers the phone, greets customers, takes water utility payments, and records them in their system. All other responsibilities belong to the Town Clerk.

Facts Provided to Participants

Discussion Prompts

Risks / Red Flags

Recommended Controls

Facilitator Notes / Expected Takeaways



Transaction Walkthrough Scenario

Participants follow a purchase from request through payment and financial reporting.

Scenario Background

Public Works Supervisor makes a purchase at the local hardware store. He asked the Store Clerk to charge it to the City's account. The purchase included a set of new doors for the warehouse which was \$1,700 and other supplies which totaled \$550. The total spent was \$2,250. Accounting received a statement from the local hardware store after the end of the month and is still waiting for a copy of the receipt of purchase from the Public Works Supervisor.

Facts Provided to Participants

Discussion Prompts

Risks / Red Flags

Recommended Controls

Facilitator Notes / Expected Takeaways



Control Failure Case Study

Participants review a cash, payroll, purchasing card, or vendor issue and identify control breakdowns.

Scenario Background

The current purchasing policy includes the use of purchasing card for purchases under \$5,000. All purchases for services require a purchase order or contract agreement. Many of the departments have began using their purchasing card to pay monthly statements rather than requesting payments through accounts payable for a check or ACH to be initiated. This has led to delays in p-card payments due to lack of documentation, lack of timely reconciliations, increased volume in p-card transactions, and corrections in accounting to general ledger from mis coding of transactions.

Facts Provided to Participants

Discussion Prompts

Risks / Red Flags

Recommended Controls

Facilitator Notes / Expected Takeaways



Internal Control Action Plan

Participants convert discussion into practical next steps for their own organization.

Scenario Background

Choose One Scenario in your own entity and Identify next steps

Facts Provided to Participants

Discussion Prompts

Risks / Red Flags

Recommended Controls

Facilitator Notes / Expected Takeaways



REFERENCES

2017 COSO ERM Integrating with Strategy and Performance
COSO Internal Control Integrated Framework Executive Summary
<https://www.coso.org>



#SOGF2026

Q&A



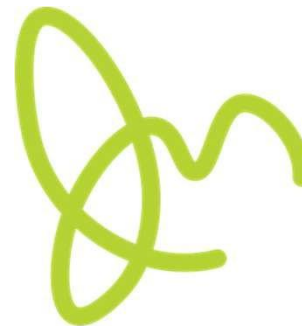
#SOGF2026

Contact Information:

Lorrie Brinson, CPA, CGFO, MBA/PA
Manager, Governmental Advisory Services
James Moore & Co.

Lorrie.Brinson@jmco.com

(352) 378-1331



**JAMES
MOORE**

