SAO

STATE ACCOUNTING OFFICE

Internal Controls and Fraud

Rachael Krizanek

Chief Compliance Officer

May 19, 2025

Agenda

- What is SAO and what does SAO do?
- Internal Controls
- Internal Control Guidance
- Internal Control Specifics
- Internal Control Sample Process
- Key Control Activity: Separation of Duties
- Key Control Activity: Reconciliations
- Internal Controls and Fraud
- Resources

Who Am I?

- Rachael Krizanek – Chief Compliance Officer at State Accounting Office (SAO)
  - Establishes and monitors statewide internal control guidance and vendor maintenance.
  - Also responsible for accounting and business process policies, along with federal Georgia reports including the Single Audit and Statewide Cost Allocation Plan (SWCAP).
  - Over 25 years of experience working with internal controls in various levels of government.

What is SAO and what does SAO do?

State Accounting Office

- The State Accounting Office is responsible for the following duties:
    - Prepare the state’s Annual Comprehensive Financial Report (ACFR); the annual audited financial statement for the entire state entity. Provide statewide financial information on interim basis.
    - Establish statewide accounting and reporting standards and practices.
    - Improve accountability, efficiencies and internal controls.
    - Train state accounting and payroll personnel in new policies, procedures and standards.
    - Operate and improve statewide financial and human capital management systems.

Statewide Reports

- Annual Comprehensive Financial Report (ACFR) – Overview and analysis of the financial activities of the State.

- Budgetary Compliance Report (BCR) – Provides information concerning financial compliance with the Amended Appropriations Act.

- Single Audit Report – Contains the Schedule of Expenditures of Federal Awards (SEFA), along with responses and corrective action plans for audit findings.

- Statewide Cost Allocation Plan (SWCAP) – Process for central service costs to be identified and assigned to benefitted activities, on a reasonable and consistent basis.

Statewide Reports

WHERE DOES THE DATA COME FROM?

- State’s Financial Software (Teamworks)
- Accounting records of the State Organizations (Agency, Authority, RESA, etc.)
- Other supplemental data gathered by SAO

Statewide Reports

WHAT ARE THEY USED FOR?

- Summarization of financial activities for the State
- Bond rating purposes
- Financial planning purposes
- Federal Compliance

Internal Controls

Internal Controls

WHAT IS IT?

- A process that provides reasonable assurance that the *objectives of the organization will be achieved*.

- Not *one event, but a series of actions* that occur throughout an organization’s operations.

- An *integral part of the operational processes* and not a separate system.

Internal Controls

RESPONSIBILITY

- Everyone has a responsibility for internal controls
  - Management – Directly responsible for the design, implementation, and operating effectiveness
  - Staff – Help management and are responsible for reporting issues
- Auditors are not considered part of an organization’s internal control system

Importance

- Effective internal controls provides reasonable assurance that objectives of the organization will be achieved:
  - Accurate accounting records and financial reports
  - Accuracy of the reports are needed to maintain fiscal health
  - Helps to reduce fraud and safeguard assets

- In government, we are ultimately protecting and serving the taxpayer

Internal Control Guidance

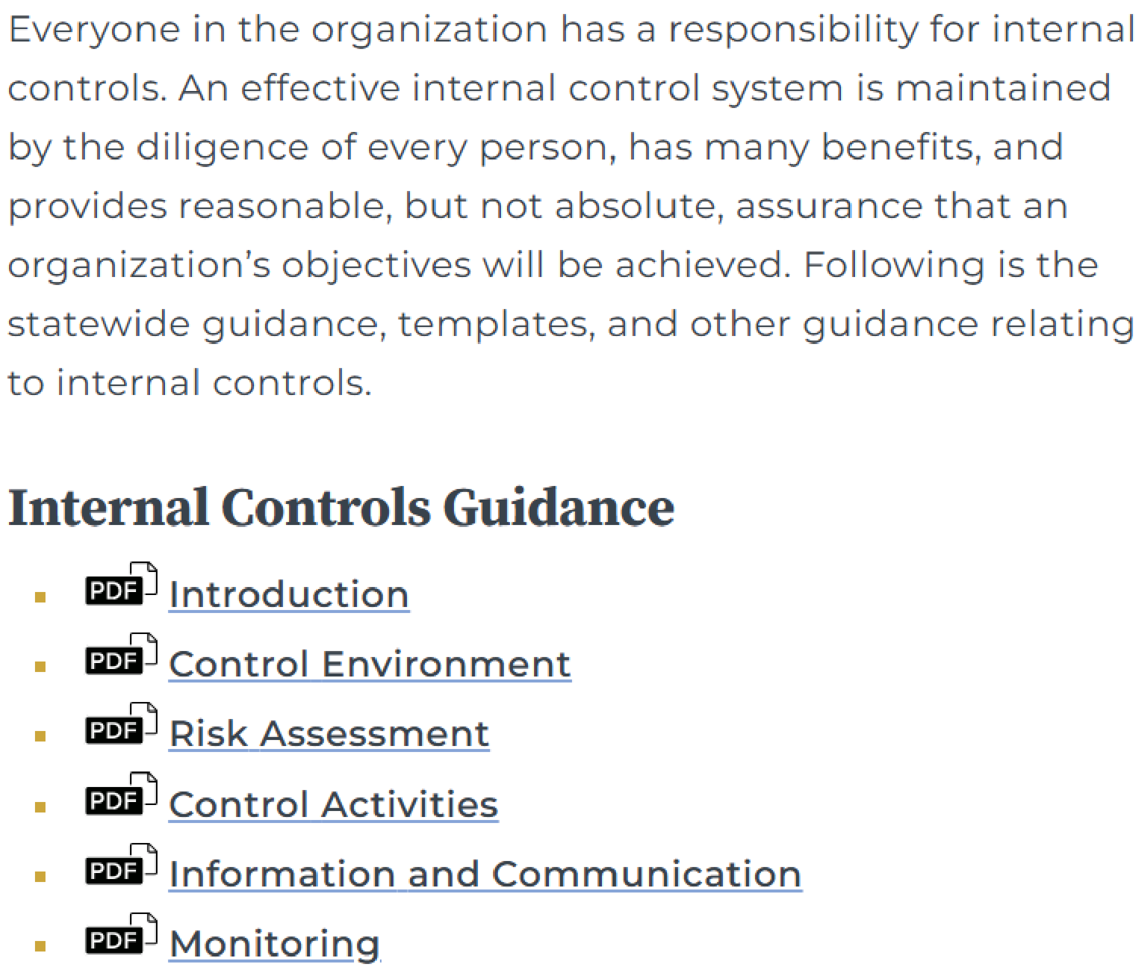
Statewide Internal Control Guidance

- SAO’s framework will provide general guidance, but it will not prescribe specifically how management should design, implement, and operate their internal control system

- Is based on Green Book, including:
  - General oversight (contained in 5 guidance chapters)
  - Georgia specific examples
  - Suggested templates (relating to financial reporting)

https://sao.georgia.gov/internal-controls

Statewide Internal Control Guidance



Everyone in the organization has a responsibility for internal controls. An effective internal control system is maintained by the diligence of every person, has many benefits, and provides reasonable, but not absolute, assurance that an organization's objectives will be achieved. Following is the statewide guidance, templates, and other guidance relating to internal controls.

Internal Controls Guidance

- PDF Introduction
- PDF Control Environment
- PDF Risk Assessment
- PDF Control Activities
- PDF Information and Communication
- PDF Monitoring

Statewide Guidance Chapters
(on SAO's website)

Where else is Internal Controls Guidance?

- Located in a variety of sources:
  - Statewide or Board guidance
  - Policies (Statewide or Board and Organization specific)
  - Procedures (Statewide or Board and Organization specific)
  - Official Code of Georgia Annotated (O.C.G.A.)
  - Etc.

Statewide Policies

- Accounting Policy Manual
  - High-level policies and procedures to ensure that financial activity is recorded accurately and consistently across organizations.
  - Basic guidance on accounting requirements, including journal entry examples, is included in these documents.
  - Accounting manual topics apply to all State of Georgia accounting organizations regardless of their accounting systems.

- Business Process Policies
  - Contains Georgia specific guidance to assist users with managing various accounting operational processes such as budget, cash, disbursements, payroll, and receivables, etc.

https://sao.georgia.gov/policies-and-procedures

Internal Control Specifics

Control Environment

- Provides the discipline and structure, which impacts the overall quality of internal controls

- Includes, such things as:
    - Code of Ethics
    - Conflicts of Interest
    - Applicable Board Rules or Law (such as OCGA sections) relating to code of ethics and conflicts of interest
    - Employment practices
    - Etc.

Risk Assessment

- Every organization faces a variety of risks from external and internal sources that impact the achievement of the organization’s objectives (such as a financial reporting objective)

- Consider what risks will get in the way of accomplishing the objective
  - Break down into specific risks, as necessary

- Need to consider risks for fraud, Information System (IT) and outsourced tasks too!

Risk Assessment

- Ultimately, the risk and change responses become internal controls (control activities) that management places into operation

- Brainstorm with personnel responsible for that specific risk example to assess risks and determine ways to reduce the level of risks

Risk Likelihood

- Level of possibility that a risk will occur:

- Without considering the known control activities (internal controls) actually occurring, analyze how likely the specific risk would be

- Certain factors to contemplate could be:
  - Ease of access to asset
  - Liquidity of the asset
  - Manual vs. automated processing
  - Etc.

Risk Impact

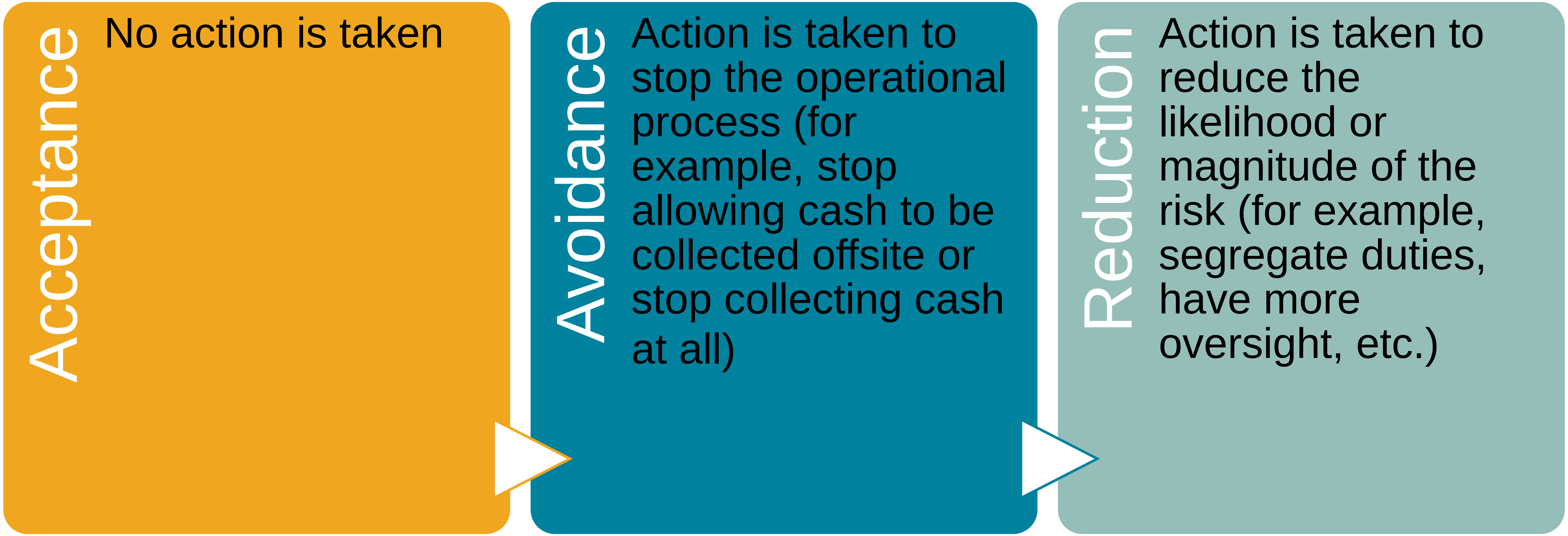
- Scale of the deficiency that could result from the risk

- Without considering the known control activities (internal controls) actually occurring, analyze what the scale of the specific risk would be

- Certain factors to contemplate could be:
  - Size
  - Pace
  - Duration
  - Etc.

Risk Responses

Management designs risk responses to respond to the analyzed risks. Responses could include:



Acceptance

No action is taken

Avoidance

Action is taken to stop the operational process (for example, stop allowing cash to be collected offsite or stop collecting cash at all)

Reduction

Action is taken to reduce the likelihood or magnitude of the risk (for example, segregate duties, have more oversight, etc.)

Control Activities

Actions management establishes through policies and procedures to achieve objectives and respond to risks (including fraud risks) in the internal control system

- Essentially, these are the tasks already being performed
- Remember this also includes information systems (computer/automated) considerations
- Essentially it is documenting all tasks that are performed with specifics such as:
  - Who does it?
  - What is done?
  - When is it done?
  - How often is it done?
  - Who reviews it?

Control Activities

PREVENTIVE VS. DETECTIVE

- Control activities can be either preventive or detective, with the main difference being the timing:

Preventive

Prevents errors from occurring, and preventing these errors helps an organization achieve an objective or addresses a risk (for example, requiring multiple levels of approval for a transaction)

Detective

Detects errors or irregularities after it occurs (for example, bank reconciliations)

Control Activities

AUTOMATED VS. MANUAL

Control activities can be implemented in either an automated or manual manner:

Automated

Either wholly or partially automated through the organization’s information technology (for example, automated validity and edit checks)

Manual

Performed by individuals with minor use of the organization’s information technology (for example, independent review)

Automated control activities tend to be more reliable because they are less susceptible to human error and are typically more efficient.

Control Activities Details

- You want to make sure you have captured the entire process in detail, such as:
    - Documenting all control activities/tasks that are performed with specifics such as:
        - Who does it?
        - What is done?
        - When is it done?
        - How often is it done?
        - Who reviews it?
        - Etc.

Control Activities Details

- Why does it matter if control activities are captured with details?

  - Control activities will be “monitored” going forward
    - Want to make sure you are monitoring the right things

  - Control activities document what tasks are actually occurring in response to risk ratings
    - Need to assess if risks are being reduced
    - If risks are not reduced:
      - There should be some sort of mitigating control activity in place (this mitigating control would be an example of a control activity to be added in your survey)

        OR

      - There should be a plan to close that gap (by implementing the missing control activity)

Control Activities

COMMON CATEGORIES

- Segregation of duties
  - Assigning key duties and responsibilities to different personnel to reduce the risk of error, misuse, or fraud
    - Example: one person initiates, a different person records, a different person approves, etc.

- Accurate and timely recording of transactions
  - Accurate – proper State expense, approved to be entered, recorded at the correct amount, in the correct account, etc.
  - Timely – within the established timeframe,
    - Example: bank reconciliations done within one week of month end, etc.

Control Activities

COMMON CATEGORIES

- Proper execution of transactions
  - Authorizing and executing transactions only by persons possessing proper authority
    - Example: does the approver verify it is a proper State purpose (such as expense), supported by documentation, received, etc.

- Reconciliations
  - Comparing balances in the accounting records to source documents (such as cash balances recorded as compared to the bank statement), and following up on any differences timely (no "plug" amounts)

Control Activities

OTHER COMMON CATEGORIES

- Controls over information processing
- Physical controls over vulnerable assets
- Access restrictions to and accountability for resources and records
- Appropriate documentation of transactions and internal controls
- Establishment and review of performance measures and indicators
- Reviews by management at the functional or activity level
- Top-level reviews of actual performance
- Management of personnel

Information and Communication

- Pertinent information must be identified, captured, and communicated in a form and timeframe that enables people to carry out their responsibilities.

- Everyone must understand their role in the internal control system, as well as how individual activities relates to the work of others.

- This component is intertwined with all aspects of the internal system.

Monitoring

- Essential in helping internal controls to remain aligned with changing objectives, environment, laws, resources, and risks.

- Assesses the quality of performance over time and promptly resolves the findings of audits and other reviews.

- A deficiency exists when a control does not operate as designed, or when the person performing the control does not possess the appropriate authority or competence.

- Corrective actions relating to the internal control system are a necessary complement to control activities to achieve objectives.

Internal Control Sample Process

Overview of the Process

- Start by establishing objectives
    - Such as financial reporting
        - “The accounting records comply with Standards and are complete and accurate”

- Then identify risks getting in way of accomplishing those objectives (risk assessment component)
    - Risk: Key assets are not all recorded at the proper amount, in the proper fund, in the proper account code or in the proper basis of accounting.
        - Assess rating and justification for inherent, likelihood and impact

- Consider how much risk are you willing to allow (risk tolerance)

Overview of the Process

- Consider “risk responses” already in place

- Document control activities (common tasks)

- Do any of those control activities offset the risk
    - If residual risk remains, need to consider response (which could be doing nothing)

- Then continuously monitor the overall internal control system (monitoring component)
    - Management is responsible for monitoring (not Auditors)
    - Determine if the controls were :
        - applied at relevant times
        - in a consistent manner
        - applied by proper person (competent, independent, etc.)

Key Control Activity: Separation of Duties

What is Separation of Duties?

- Designing control activity (job) responsibilities so incompatible duties are separated

- Key preventive control for many risk areas, to help reduce errors, misstatement, theft, fraud, etc.

- Management considers the need to separate control activity responsibilities related to authority, custody, and accounting of operations to achieve adequate separation of duties

- If separation of duties is not practical because of limited personnel or other factors, management designs alternative control activities to address the risk of fraud, waste, or abuse in the operational process

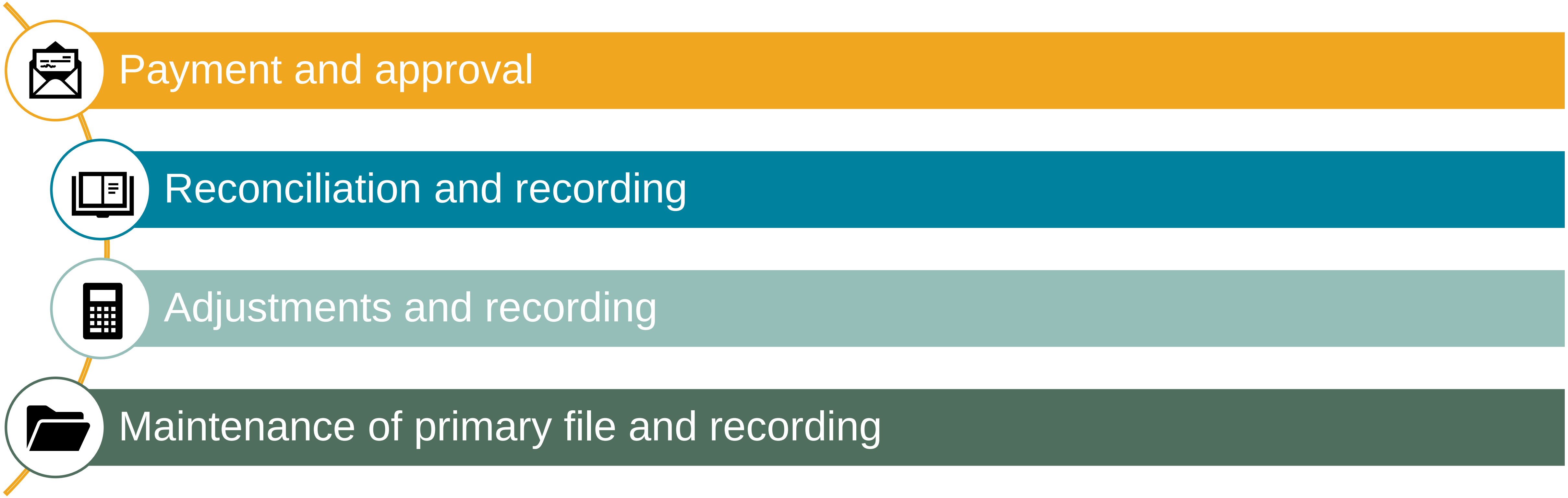
Separating Key Duties

- Management designs control activities so not one individual controls all aspects of a cycle. Some possible ways to do this could include:
  - Having someone approve or perform the transaction.
  - Having a different person record the transaction.
  - Having a *different person prepare applicable reconciliations* relating to the transaction.
  - Having a different person prepare any reports relating to the transaction.

- Management designs mitigating control activities if separation of duties is not possible. Some possible ways to do this could include:
  - Having a *different person* verify the work performed by the first person.
  - Having increased review or supervision by management (not involved in the process).

Key Disbursement Steps to Separate

If it is not practical to separate all disbursement duties, certain key categories should be separated:



- Payment and approval
- Reconciliation and recording
- Adjustments and recording
- Maintenance of primary file and recording

Sample Mitigating Controls for Disbursements

Management must implement mitigating controls if key duties are not separated, such as:

- Outsourcing or using central shared services for certain disbursement steps, such as:
    - Payroll Services
    - Check printing
    - Vendor maintenance
- Cross-train employees from other functional departments to perform reconciliations or certain disbursement duties
- Routine monitoring via audit logs or other reports of transactions entered and/or processed
- Additional supervisory or internal audit reviews, including review of supporting documentations or transaction logs, reports, data analytics (performance measures, indicators, etc.), and reconciliations
- Require employees who are involved in incompatible disbursement duties to take routine time off and/or rotate duties performed
    - Temporarily remove system access during this time

Key Receipts Steps to Separate

If it is not practical to separate all receipts duties, certain key categories should be separated:

- Billing and recording
- Collecting and recording
- Reconciliation and recording
- Adjustments and recording
- Adjustments and collecting
- Maintenance of primary customer file and recording

Sample Mitigating Controls for Receipts

Management must implement mitigating controls, if key duties are not separated, such as:

- Outsourcing or using central shared services for certain receipts steps, such as:
  - Lockbox
- Cross-train employees from other functional departments to perform reconciliations or certain receipt related duties.
- Routine monitoring via audit logs or other reports of transactions entered and/or processed.
- Additional supervisory or internal audit reviews, including review of supporting documentations or transaction logs, reports, data analytics (performance measures, indicators, etc.), and reconciliations.
- Require employees who are involved in incompatible receipt related duties to take routine time off and/or rotate duties performed.
  - Temporarily remove system access during this time

Key Control Activity: Reconciliations

What is a Reconciliation?

Comparing a balance in the accounting records to a source document and following up on any differences. Some examples of reconciliations include:

Bank Reconciliation

Comparing amount of cash in accounting records to bank cash balance.

Control Account Reconciliation

Comparing of amounts in subsidiary ledger (ex: customer accounts) to general ledger control account (ex: accounts receivable) balance.

Clearing Account Reconciliation

Reconciling amounts in the clearing account (which accumulates transactions which are later distributed to appropriate accounts.

Why are Reconciliations so Important?

Reconciliations are the most important detective control activity that:

- Confirms that transactions are being processed, recorded, and accounted for completely and accurately
- Determines whether the transactions are recorded properly, have yet to be recorded, or were recorded improperly and require correction
- Serves to identify unauthorized transactions and explain differences

They help to support the accuracy of the accounting records and ultimately lead to more reliable financial reports.

Bank Reconciliation Steps

- Necessary steps that *must be* done during the bank reconciliation process:
  - Verify ending bank balance agrees to balance per the accounting records (for the same date)

  - If the balances do not agree determine the reasons for differing amounts, such as:
    - Outstanding checks
    - Deposits in transit
    - Other reconciling items (such as wire transfer performed, but not entered in the general ledger)

Control Account Reconciliation Steps

Necessary steps that *must be* done during the control account reconciliation process:

- Verify the general ledger control account amount (ex: accounts receivable or accounts payable) agrees to the sum total of amounts in subsidiary ledger (ex: customer accounts or benefit payees).

- If the balances do not agree determine the reasons for differing amounts, such as:
  - Unrecorded transactions
  - Different amounts recorded/posted
  - Timing differences between systems
  - Errors in calculations or integrations

Reconciling Items Impact

- What are the impacts of not researching and resolving reconciling items in the various reconciliations?
    - The reconciliation is <u>not actually complete</u>
    - Errors in the accounting records are not discovered and corrected timely, such as:
        - Transactions not recorded
        - Amounts not recorded at the correct amount
        - Amounts recorded but the transaction did not actually occur
    - Fraud occurring that is not being detected (or not detected timely)
    - Impact to audit opinions on financial statements (including Statewide reports)
    - Audit Findings

Internal Controls and Fraud

Types of Fraud

Consider the types of fraud that can occur:

- Fraudulent financial reporting - Intentional misstatements or omissions of amounts or disclosures in financial statements to deceive financial statement users
  - This could include intentional alteration of accounting records, misrepresentation of transactions, or intentional misapplication of accounting principles
- Misappropriation of assets - Theft of assets, such as theft of property, embezzlement of receipts, or fraudulent payments
- Corruption - Bribery and other illegal acts

Also consider misconduct that can occur, such as waste and abuse.

Fraud Risk

- Analyze and respond to identified fraud risks so that they are effectively mitigated

- Fraud risks are analyzed through the same risk analysis process performed for all identified risks

- Management considers fraud risk factors
  - Fraud risk factors do not necessarily indicate that fraud exists but are often present when fraud occurs

- Analyze the identified fraud risks by estimating their significance, both individually and in the aggregate, to assess their effect on achieving the defined objectives
  - Also, assess the risk of management override of controls

Fraud Risk Factors

Incentive/pressure

Management or other personnel have an incentive or are under pressure, which provides a motive to commit fraud

Opportunity

Circumstances exist, such as the absence of controls, ineffective controls, or the ability of management to override controls, that provide an opportunity to commit fraud

Attitude/rationalization

Individuals rationalize committing fraud. Some individuals possess an attitude, character, or ethical values that allow them to knowingly and intentionally commit a dishonest act

Internal Controls and Fraud

Respond to fraud risks through the same risk response process performed for all analyzed risks.

- Design an overall risk response and specific actions for responding to fraud risks

Control activities to help prevent fraud (by reducing or eliminating certain fraud risks) could include:

- Separation of duties
- Reconciliations
- Documentation review/verification (especially to original source of data)
- Independent verification
- Data analysis trends (such as unexplained increase in the count or dollar amount of transactions)

Fraud – Next Steps

After a fraud or loss occurs, the internal control process should be reviewed to determine if:

- Internal controls were designed properly, however, they were not executed as designed
- Design of the internal control system needs to be updated to mitigate a risk that was discovered (i.e., reason the fraud or loss had occurred)

Common Fraud Examples

Inappropriate Payments

- Payment to an inappropriate/fictious vendor
  - Vendor does not exist
  - Vendor address was changed
  - Payee name was changed on the check

- Payment to an inappropriate bank account
  - Bank account was inappropriately changed on existing vendor

Fraud Mitigating Controls

Control activities to help prevent fraud (by reducing or eliminating certain fraud risks) could include:

Separation of duties

- Who can enter payments?
- Who can add or edit vendors/payees?
- Is someone not involved in part of the payment process verifying the good/service was received?
- Who can approve payments?
- Who releases payments?

Reconciliations

- Are bank reconciliations performed timely?
- Are there unexplained adjustments or “plugs”?
- Is the person doing the reconciliation not part of the payment process?

Documentation review / verification

- Is someone reviewing legitimacy of the invoice?

Data analysis trends

- Someone reviewing for unexplained increases in the count or dollar amount of transactions to that expense.
- Are there a lot even (or same) dollar amount payments suddenly?

Common Fraud Examples

Procurement of items (assets)

- Items purchased only from known people
- Items purchased and delivered elsewhere
- Items stolen and not returned

SAO

Fraud Mitigating Controls

Control activities to help prevent fraud (by reducing or eliminating certain fraud risks) could include:

Separation of duties

- Who can request purchase of items?
- Who can add or edit vendors?
- Is someone not involved in part of the purchase process verifying the good/service was received?
- Who is recording the purchase of the item in the accounting or inventory records?

Inventories

- Are items tagged?
- Are physical inventories performed routinely?
- Are there unexplained adjustments”?
- Is the person doing the physical inventory not part of the purchase process?

Documentation review / verification

- Is someone reviewing legitimacy of the receiving document, invoice, etc.?

Data analysis trends

- Someone reviewing for unexplained increases in the count or dollar amount of transactions to that expense.

Resources

Resources

Green Book

- https://www.gao.gov/greenbook

SAO's website:

- https://sao.georgia.gov/policies-and-procedures
- http://sao.georgia.gov/internal-controls
- https://sao.georgia.gov/swar/acfr
- https://sao.georgia.gov/swar/bcr
- https://sao.georgia.gov/swar/federal-compliance-reporting

Contact Information:

- Compliance@sao.ga.gov
- Rachael.Krizanek@sao.ga.gov