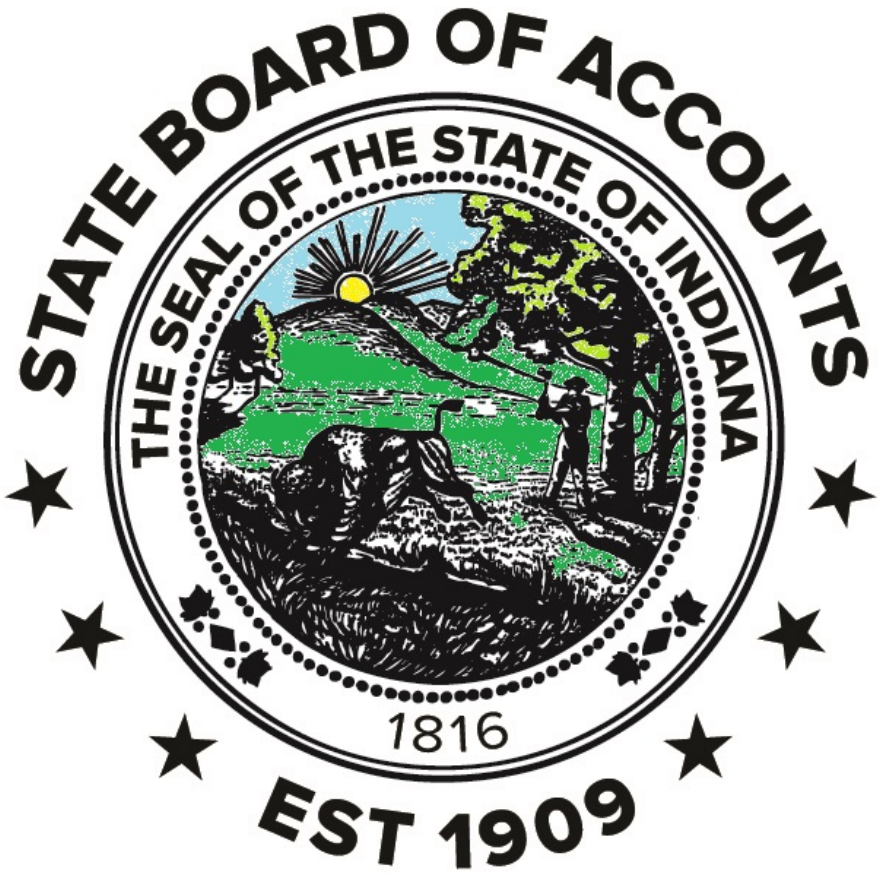
# UNIFORM INTERNAL CONTROL STANDARDS FOR INDIANA POLITICAL SUBDIVISIONS




Paul D. Joyce, CPA
State Examiner

September 2015

# STATE OF INDIANA

**AN EQUAL OPPORTUNITY EMPLOYER**

STATE BOARD OF ACCOUNTS
302 WEST WASHINGTON STREET
ROOM E418
INDIANAPOLIS, INDIANA 46204-2769

Telephone: (317) 232-2513
Fax: (317) 232-4711
Web Site: www.in.gov/sboa


## A MESSAGE FROM THE STATE EXAMINER, PAUL D. JOYCE

My Fellow Public Servants:

Indiana Code 5-11-1-27 requires each political subdivision to maintain a system of internal control to promote government accountability and transparency. As a result, the State Board of Accounts has developed the *Uniform Internal Control Standards for Indiana Political Subdivisions,* which provides a basis of common understanding to assist public sector managers in this effort. This manual defines what an internal control system is and against what standards your system is measured when evaluated for sufficient controls. Our goal is to work with you in partnership to achieve a system of controls that will be instrumental in ensuring that all public officials and employees serve the people with responsibility, integrity, loyalty, and efficiency.

Paul D. Joyce

Paul D. Joyce, CPA
State Examiner

# Table of Contents

# Introduction

Indiana Code 5-11-1-27 provides that internal control standards shall be defined to promote government accountability and transparency. This statute applies to all political subdivisions under IC 5-11-10.5-1, including counties, townships, cities, towns, school corporations, library districts, fire protection districts, public transportation corporations, local hospital authorities or corporations, local airport authority districts, special service districts, special taxing districts, or other separate local governmental entities that may sue and be sued.

The State Board of Accounts (SBOA) is required under Indiana Code 5-11-1-27(e) to define the acceptable minimum level of internal control standards. To provide clarifying guidance, the State Examiner compiled the standards contained in this publication: *Uniform Internal Control Standards for Indiana Political Subdivisions*. These standards have been based on those advocated by leading authorities in the field of internal control. All political subdivisions subject to audit by SBOA are expected to adhere to these standards, and will be evaluated accordingly in any audits that are performed by or on behalf of the SBOA.

Internal control is a process executed by officials and employees that is designed to provide reasonable assurance that the mission and objectives of the organization will be achieved. The internal control process includes any policy, system, or action that corresponds directly to the objectives of the organization and adjusts to change when necessary.

In government, missions and objectives change and evolve as a result of various factors such as new management, change in staff, rapid growth, technological advances, and new programs or services. As missions and objectives change, internal controls must be monitored and evaluated for applicability in the new context and adjusted accordingly. Often, new internal controls are implemented without a corresponding deletion in obsolete controls. Maintaining processes which have no clear purpose fosters confusion and ineffective utilization of resources, resulting in a control weakness. Therefore, internal controls should be identified, monitored, and evaluated on a continual basis.

Ultimately it is the people at every level of the organization that are instrumental in ensuring the success of the internal control process. Accordingly, internal controls integrate the attitudes and actions of people within the organization into the processes.

There are many benefits of a well-defined, relevant internal control process. The process produces accountability and transparency that is evident both internally and externally. Internally, the accomplishment of objectives may be quickly evaluated; any inefficiency may be addressed and corrected immediately. Internal control procedures encourage efficient uses of

# Introduction

government time and resources through the establishment of baselines and other measurable goals. Measurable goals and objectives allow the government to externally communicate success in the performance of missions and objectives. Moreover, the government may convey to the public its commitment to detect and eliminate fraud, waste, and abuse. Internal control procedures reduce costs by enabling timely completion of responsibilities as well as prevention of waste, abuse, or fraud. Additionally, audit costs are reduced as documented processes exist to reasonably ensure that operational, reporting, and compliance objectives are achieved. Finally, the inherent savings and goodwill fostered with the citizens through proper stewardship of their assets is immeasurable.

The internal control process is based on well-established and widely-recognized fundamental principles that operate as an integrated whole but are best understood when analyzed individually. The five components that are recognized as basic to any internal control system are listed in IC 5-11-1-27(d), as follows: Control Environment, Risk Assessment, Control Activities, Information and Communication, and Monitoring. Additionally, the Committee of Sponsoring Organizations of the Treadway Commission COSO provides a framework that includes principle characteristics of these five components and three categories of generalized objectives. The U.S. Government Accountability Office has adapted these components and principles for the Federal government through its *Standards for Internal Control in the Federal Government*, otherwise known as the "Green Book." Accordingly, this SBOA publication is organized on the basis of these conceptual frameworks.

Part One - Minimum Level of Internal Control Standards: This part defines and details the minimum standards through which the system of a political subdivision will be evaluated for sufficient internal controls.

Part Two - Approved Personnel Training Materials: This part contains materials related to the video presentation by the State Board of Accounts on Internal Control. Also included in this section are examples of internal control procedures that could be used to meet each of the seventeen principles. Lastly, this part provides case studies of deficiencies found in SBOA audits and possible resolutions through controls. Please remember, every situation is different and will call for its own unique internal control process. There is no one static internal control process.

Because governments vary in size and complexity, no single method or set of internal control policies and procedures is universally applicable. While this manual provides minimum requirements, internal control is a dynamic open field, with information and publications that might be beneficial in helping the user tailor controls to better fit the organization's particular

# Introduction

needs. While adoption of the "Green Book" is not required, we strongly suggest it as a companion guide, especially for those with oversight or internal control development responsibilities. It may be found at www.gao.gov/greenbook.

To keep informed about developments in the field of internal control, consult other professional literature, visit relevant web sites, join professional accountability organizations, and attend training programs on the subject of internal control.

**DEFINITION OF INTERNAL CONTROL**

By necessity, the definition of internal control is broad. Internal control is a conceptual process that is applied to a wide range of situations in a wide range of environments. The purpose of the internal control process is to provide reasonable assurance that the mission and objectives of an organization will be achieved. This purpose includes the reduction of risk associated with fraud as well as a safeguard of resources against loss due to waste, abuse, mismanagement, or errors. Internal control provides a check and balance system over operations, promoting operational effectiveness and efficiency. A system of sufficient internal control produces reliable financial and management data; ensures accuracy and timeliness in reporting; and promotes compliance with laws.

SBOA defines internal control as follows:

- *Internal control is a process executed by officials and employees that is designed to provide reasonable assurance that the objectives of the political subdivision will be achieved;*
- *It is a basic element fundamental to the organization, rather than a list of added on tasks;*
- *It is an adaptable process that is a means to an end, not an end in itself;*
- *It is focused on the achievement of objectives; and*
- *It is dependent on officials and employees for effective implementation.*

Each of the five components of internal control is necessary to form a complete internal control process: Control Environment, Risk Assessment, Control Activities, Information and Communication, and Monitoring Activities. If any of the five components is missing, true internal control is not achieved. Additionally, each component is comprised of recognized principle elements. To have a complete component, the principles associated with each component should be present.

# Introduction

**DOCUMENTATION OF INTERNAL CONTROL**

Documentation is a necessary part of effective internal control. Documentation relates internal control procedures to the missions and objectives of the unit, solidifies expectations, and provides an effective way to communicate the process. Management uses judgment in determining the extent of documentation needed. However, SBOA recommends the minimum documentation requirements found in the "Green Book."

**ORGANIZATIONAL ROLES**

All members of a political subdivision, including all elected officials, board members (compensated or not), and employees fulfill a role in the system of internal control. However, leadership of the political subdivision sets the tone; clear support from leadership engages a successful, effective internal control system and emphasizes the importance of contributions that each individual provides as part of the team. If leadership does not effectively establish and clearly communicate support for internal control and what the internal control system is, the political subdivision will likely experience a weak, ineffective internal control system that is only sporadically successful. While these internal control standards are useful and applicable to all members, personnel as defined under IC 5-11-1-27 have been specifically charged with understanding the standards and procedures adopted by the legislative body of the political subdivision. IC 5-11-1-27 (c) provides that personnel means, "an officer or employee of a political subdivision whose official duties include receiving, processing, depositing, disbursing, or otherwise having access to funds that belong to the federal government, state government, a political subdivision, or another governmental entity."

After June 30, 2016 the legislative body of the political subdivision must ensure that the internal control standards and procedures are adopted by the political subdivision and that personnel receive the necessary training.

**PROCEDURES FOR ADOPTION OF INTERNAL CONTROL POLICY AND TRAINING**

At a minimum, the legislative body shall stipulate in a policy that they have adopted the internal control standards as defined by SBOA under IC 5-11-1-27(e). Personnel training of individuals shall be evidenced through a certification process. The certification form that is to be used and retained by the political subdivision is found in the Appendix of this manual. The fiscal officer of a political subdivision must certify in writing that the minimum internal control standards have been adopted and personnel, not on leave status, have received training. The certification must be filed with SBOA at the same time as the Annual Financial Report is filed, beginning in 2017.

**OBJECTIVES**

The achievement of objectives is the purpose of the internal control system and so the objective(s) must first be defined. In general, objectives for political subdivisions originate from purposes and functions detailed in laws,

regulations, ordinances, etc. Objectives are set at both the entity level and at office level by the oversight body and management and must be viewed from a holistic, interrelationship approach.

There are three broad categories of objectives which help to clarify the objective setting process:

- *Operations objectives* which are designed to analyze operational and performance goals along with the effectiveness and efficiencies of operation, including the safeguarding of assets.
- *Reporting objectives* which are designed to consider both financial and non-financial information, internal and external to the unit, with an expectation of reliability, accountability and transparency.
- *Compliance objectives* which are designed to assure adherence to laws and regulations.

These objective categories are interrelated and, therefore, may overlap.

**DEFINITIONS OF OVERSIGHT BODY, LEGISLATIVE BODY, AND MANAGEMENT**

The oversight body and management work together and share responsibility for the development and implementation of internal controls for the political subdivision. Management is primarily responsible for the design and implementation of the internal control structure. The oversight body has the ultimate responsibility to oversee and monitor that the internal controls have been implemented and are being followed by the political subdivision as a whole.

The oversight body is by default the legislative body for each political subdivision. However, the legislative body can establish a separate oversight body. They would need to specify who or which positions will be part of the oversight body and what the responsibilities of the oversight body will be.

Each political subdivision has unique organization requirements and statutory authorities that define who is part of management and who is part of the legislative body.

**County**

For Counties, the legislative body is usually the Board of Commissioners. However, there are a few counties that under statute have established the County Council as the legislative body. For counties, the legislative body might want to consider establishing an oversight committee made up of representatives from the Commissioners, the Council and other office

holders or department heads. If a county legislative body chooses to establish an oversight committee, they should also establish the composition of the oversight committee and what responsibilities they are delegating to that committee.

Management includes elected officials and department heads that design and implement controls and control activities for their office or department. As much as possible, those controls should be documented and provided to all employees. Feedback between the legislative body/oversight committee and management should be established at the beginning of the internal control process.

**City or Town**

For second and third class Cities, the Common Council is the legislative body. For Towns, the Town Council is the legislative body. If the legislative body for a City or Town chooses to establish an oversight committee, they should also establish the composition of the oversight committee and what responsibilities they are delegating to that committee.

Management includes elected officials and department heads that design and implement controls and control activities for their office or department. As much as possible, those controls should be documented and provided to all employees. Feedback between the legislative body/oversight committee and management should be established at the beginning of the internal control process.

**School**

For School Corporations, the legislative body is the School Board of Trustees. If the legislative body for a School chooses to establish an oversight committee, they should also establish the composition of the oversight committee and what responsibilities they are delegating to that committee.

Management is a combination of the Superintendent and the Finance Director (CFO, Business Manager, Treasurer, etc.) who design and implement internal controls and control activities for the School Corporation. As much as possible, those controls should be documented and provided to all employees. Feedback between the legislative body and management should be established at the beginning of the internal control process.

For Extra-Curricular Accounts, the legislative body is the School Board of Trustees. If the legislative body for the Extra-Curricular Accounts chooses to establish an oversight committee, they should also establish the composition of the oversight committee and what responsibilities they are delegating to that committee.

# Introduction

Management is a combination of the Superintendent, the Finance Director (CFO, Business Manager, Treasurer, etc.), the School Principal, and the ECA Treasurer who design and implement internal controls and control activities for the Extra-Curricular Accounts. As much as possible, those controls should be documented and provided to all employees. Feedback between the legislative body and management should be established at the beginning of the internal control process.

**Township**

For Townships, the legislative body is the Township Board. If the legislative body for a Township chooses to establish an oversight committee, they should also establish the composition of the oversight committee and what responsibilities they are delegating to that committee.

Management is the Township Trustee who designs and implements internal controls and control activities for the Township. As much as possible, those controls should be documented and provided to all employees. Feedback between the legislative body and management should be established at the beginning of the internal control process.

**Other Governmental Units**

For a governmental unit not previously discussed and defined, the governing body of the unit is the legislative body. If the legislative body for another governmental unit chooses to establish an oversight committee, they should also establish the composition of the oversight committee and what responsibilities they are delegating to that committee.

Management includes elected and/or appointed officials and department heads that design and implement controls and control activities for their office or department. As much as possible, those controls should be documented and provided to all employees. Feedback between the oversight body and management should be established at the beginning of the internal control process.

# Part One:

# Minimum Level of Internal Control Standards

# FIVE COMPONENTS OF INTERNAL CONTROL

A system of internal control may be implemented in many different ways. Because political subdivisions vary in purpose, size and complexity, no single method of internal control is universally applicable. However, the five internal control components and seventeen principles should be present and functioning, operating in an integrated manner. Some components may have principles implemented entity-wide, which impact the internal control system for all objectives, while other components may be specific to a given objective.

The terms oversight body and management are used throughout these guidelines. Please refer to the Introduction Section for the definitions appropriate to your political subdivision.

**Component One: Control Environment**

The control environment is the basic commonality for all and comprises the integrity and ethical values of the political subdivision established by the oversight body and management. The standards, processes, and structures which form the control environment pervasively impact the overall system of internal control. The oversight body and management convey leadership expectations, and overall tone which are reinforced by all officials and management throughout the various offices and departments. The control environment also contains the overall accountability structure for all employees through performance and reward measures. Within this structure, leadership demonstrates commitment to the political subdivision by having a process for attracting, developing, and retaining competent individuals. This component is static in that its underpinnings do not generally change with a given objective.

Five of the seventeen principles of internal control pertain to the control environment:

**Principle 1. The oversight body and management demonstrate a commitment to integrity and ethical values.**

The oversight body and management demonstrate these values through directives, attitudes and behavior. Established standards of conduct are expected to be observed by all throughout the political subdivision and are used when evaluating adherence to the values of the political subdivision.

**Principle 2. The oversight body oversees the entity's internal control system.**

There is an oversight structure in place. The oversight body oversees management's design, implementation, and operation of the political subdivision's internal control system.

# FIVE COMPONENTS OF INTERNAL CONTROL

**Principle 3. Management establishes an organizational structure, assigns responsibility, and delegates authority to achieve the political subdivision's objectives.**

Organizational structure is designed, responsibilities are assigned and authority delegation is identified to enable the political subdivision to plan, execute, control and assess achievement of objectives. The organizational structure is designed so that it is clear where responsibilities are, especially for those areas where statute has not assigned particular responsibilities. When needed, management will go back to the legislative body to enact the policies that will clearly define these areas, specifically when the organizational structure extends beyond office or department boundaries to affect the political subdivision as a whole. Management develops and maintains documentation of the internal control system.

**Principle 4. Management demonstrates a commitment to attract, develop and retain competent individuals.**

Policies pertaining to the recruitment, training, mentoring, and retention of personnel consider the objectives of the political subdivision, including succession and contingency plans for key roles.

**Principle 5. Management evaluates performance and holds individuals accountable for their internal control responsibilities.**

Individuals are held accountable for their internal control responsibilities through a recognized, understood structure which includes corrective action procedures. Additionally, management evaluates for excessive pressures on personnel and adjusts these pressures accordingly.

**Component Two:**
**Risk Assessment**

Risk is the possibility that an event will occur and adversely affect the achievement of objectives. Risk assessment is the process used to identify and assess internal and external risks to the achievement of objectives, and then establish risk tolerances. Each identified risk is evaluated in terms of its impact and likelihood of occurrence. Overall, risk assessment is the basis for determining how risk will be managed.

Four of the seventeen principles of internal control apply to risk assessment:

# FIVE COMPONENTS OF INTERNAL CONTROL

**Principle 6. Management defines objectives clearly to enable the identification of risks and defines risk tolerances.**

Objectives defined in clear terms will include information such as: who is to achieve the objective, how the objective will be achieved, and when the objective will be achieved.

**Principle 7. Management identifies, analyzes, and responds to risk related to achieving the defined objectives.**

Management identifies risks to the achievement of the political subdivision's objectives across the unit as a whole and within each office or department. Analysis of risk through determination of objective measures and variance tolerances is the basis for determining how the risks should be managed. The response to risk is selected: acceptance, avoidance, reduction, or sharing.

**Principle 8. Management considers the potential for fraud when identifying, analyzing, and responding to risks.**

The types of fraud which could impact the achievement of objectives include fraudulent financial reporting, misappropriation of assets, and corruption. As a part of this analysis, fraud risk factors are identified: pressure, opportunity, and rationalization. The response to fraud risk exercises the same process used for all analyzed risks.

**Principle 9. Management identifies, analyzes, and responds to significant changes that could impact the internal control system.**

Internal control is a process, and part of that process is the responsibility for management to be continually aware of changes, both external and internal, that could affect the achievement of the political subdivision's objectives. Those changes should be analyzed for both their immediate effect and for any future impact. Management would then determine any modifications needed in the internal control process to adapt to these changes.

**Component Three: Control Activities**

Control activities are the actions and tools established through policies and procedures that help to detect, prevent, or reduce the identified risks that interfere with the achievement of objectives. Detection activities are designed to identify unfavorable events in a timely manner whereas prevention activities are designed to deter the occurrence of an unfavorable event. Examples of these activities include reconciliations, authorizations, approval processes, performance reviews, and verification processes.

# FIVE COMPONENTS OF INTERNAL CONTROL

An integral part of the control activity component is segregation of duties. The fundamental premise of segregation of duties is that an individual or small group of individuals should not be in a position to initiate, approve, undertake, and review the same action. Separating the ability to record, authorize, and approve the transactions along with the handling of the related asset reduces the risk of error or fraudulent actions. It also reduces the risk of management override.

In very small governmental units, such segregation may not be practical. In this case, compensating activities should be implemented which may include additional levels of review for key operational processes, random and/or periodic review of selected transactions. These additional levels of review may take the form of managerial review of reports of detailed transactions, periodic review of performance of reconciliations, and periodic counts of assets and comparison to records. Certain situations may require management to go outside of the office or department for help in implementing controls and these reviews might be performed by governing boards or other elected officials.

There is an expectation of segregation of duties. If compensating controls are necessary, documentation should exist to identify both the areas where segregation of duties are not feasible or practical and the compensating controls implemented to mitigate the risk. Clear documentation should be maintained for continuity as well as ease of communication to outside parties.

Three of the seventeen principles of internal control apply to control activities:

**Principle 10. Management designs control activities to achieve objectives and respond to risks.**

Control activities are designed to fulfill defined responsibilities and address identified risks. An evaluation of the purpose of the control activity is performed as well as an evaluation of the effect a deficiency would have on objectives. Control activities may be either automated or manual. The Green Book identifies a list of control activity categories that are meant only to illustrate the range and variety of control activities; the list is by no means all inclusive, but is reproduced here for reference purposes:

- Top-level reviews of actual performance.
- Reviews by management at the functional or activity level.
- Management of human capital.

## FIVE COMPONENTS OF INTERNAL CONTROL

- Controls over information processing.
- Physical control over vulnerable assets.
- Establishment and review of performance measures and indicators.
- Segregation of duties.
- Proper execution of transactions.
- Accurate and timely recording of transactions.
- Access restrictions to and accountability for resources and records.
- Appropriate documentation of transactions and internal control.

**Principle 11. Management designs the political subdivision's information system and related control activities to achieve objectives and respond to risks.**

Control activities are designed to support the completeness, accuracy, and validity of information processing by technology including the design of security management. Management evaluates changes to systems and updates control activities in response. For example,

- Disaster Recovery ensures that critical accounting information will be processed in the event of interruption of computer processing capacity.
- Back-Up Processing provides for accounting information to be backed up on a periodic basis sufficient to allow restoration of the information in a timely manner.
- Physical Security protects the computer system and the associated telecommunications equipment from environmental damage and unauthorized access.
- Logical Security requires access to accounting information and processes be controlled by operating system software and by the computerized accounting application through user identification codes and passwords.
- Change Controls are internal controls over changes made to the accounting system's computer programs.

# FIVE COMPONENTS OF INTERNAL CONTROL

- Audit Trails allow for sufficient documentation to trace all transactions from the original source of entry into the system, through all system process, and to the results produced by the system.

- Input Controls provide input edits and controls to assure that information entered into the system is accurate, that all appropriate information is entered into the system.

- Segregation of Duties can be achieved within information technology systems by appropriate assignment of security profiles that define the data the users can access and the functions they can perform.

- Output Controls are features that assure all accounting information is reported accurately and completely.

- Interface Controls allow for Information generated in one computer application system to be transferred to another computer application system accurately and completely.

- Internal Processing provides written verification procedures and actual verification results that document accurate calculating, summarizing, categorizing, and updating of accounting information on a periodic basis.

**Principle 12. Management implements control activities through policies.**

Management works with each office or department in determining the policies necessary to address the objectives and related risks for the operational process. Further defined policies through day-to-day procedures may be warranted. These policies are periodically reviewed for continued relevance and effectiveness.

**Component Four: Information and Communication**

Relevant information from both internal and external sources is necessary to support the functioning of the other components of internal control. Communication is the continual process of providing, sharing, and obtaining necessary information. Internal communication enables personnel to receive a clear message that control responsibilities are taken seriously by the organization. External communication enables relevant outside information to be internalized and internal information to be clearly communicated to external parties.

# FIVE COMPONENTS OF INTERNAL CONTROL

Three of the seventeen principles of internal control pertain to the component of information and communication:

**Principle 13. Management uses quality information to achieve the political subdivision's objectives.**

Management defines the types of information needed and the acceptable sources of information. Then, management processes and evaluates the information for relevancy. Information should be appropriate, current, complete, accurate, accessible, and timely.

**Principle 14. Management internally communicates the necessary quality information to achieve the political subdivision's objectives.**

Information is communicated using established reporting lines. Appropriate communication methods consider the audience, nature of the information, availability, cost, and any legal or regulatory requirements.

**Principle 15. Management externally communicates the necessary quality information to achieve the entity's objectives.**

Management identifies external parties and communicates relevant information. Appropriate communication methods are developed and should include the same consideration as outlined for internal communication.

**Component Five: Monitoring Activities**

Evaluations are used to determine whether each of the five components of internal control is present and functioning. These evaluations may be conducted on an ongoing or periodic basis. The criteria used are developed by the oversight body, elected officials, management, governing boards, or recognized standard-setting bodies or regulators.

Two of the seventeen principles of internal control apply to monitoring activities:

**Principle 16. Management establishes and operates monitoring activities to monitor the internal control system and evaluate the results.**

A baseline of the current state of the internal control system is compared against the original design of the internal control system. The baseline consists of issues and deficiencies identified in the internal control system. The results of the monitoring process are evaluated and documented.

## FIVE COMPONENTS OF INTERNAL CONTROL

Potential changes to the internal control system are identified. Control and monitoring activities may be the same, but it is the intent of the activity that distinguishes which component the activity is supporting. For example, a review of reconciliation with the intent to detect errors would be a control activity while a review of the same reconciliation with the intent to determine if internal control procedures are in place and functioning properly would be a monitoring activity.

**Principle 17. Management remediates identified internal control deficiencies on a timely basis.**

Management establishes a mechanism for personnel to report internal control issues identified while performing their responsibilities. These issues are documented and evaluated on a timely basis.

Management remediates identified issues. **Corrective actions include resolution of audit findings.**

# Part Two:

# Approved Personnel Training Materials Supplement

# INTERNAL CONTROL SYSTEMS

Handouts for Video Presentation located on website www.in.gov/sboa

## INTRODUCTION

- The information on the following slides supplement and support the PowerPoint presentation on the Uniform Internal Control Standards for Indiana Political Subdivisions. This presentation is available on the State Board of Accounts website www.in.gov/sboa
- The presentation is available in webinar format to anyone who would like to review the information.

## Why do we talk about internal controls then find it difficult to take action?

- Control systems are not uniform.
- They are not tangible.

They are not rocket science but in order to be effective they have to be more than just thoughts in the mind of management.

## Summary of the Discussion

- Understanding Internal Control
  - 3 Categories of Objectives
  - 5 Components on Internal Control Systems
  - COSO/Green Book
    - Expanded guidance on the role of those in charge of governance in Internal Control Systems
    - Adjusted for increased dependence on IT
    - 17 principles under the 5 components
- Implementation

# Definition of Effective Internal Control

An effective system of internal control requires that:

- Each of the 5 components and 17 principles are present and functioning and,
- The 5 components operate together in an integrated manner.

A major deficiency exists if the county cannot conclude that these are met.

# Internal Control Framework


*Internal Control - Integrated Framework,* ©2013 Committee of Sponsoring Organizations of the Treadway Commission (COSO). All rights reserved. Used with permission.

## Management's Objectives

- Operations
- Reporting
- Compliance


*Internal Control - Integrated Framework,* ©2013 Committee of Sponsoring Organizations of the Treadway Commission (COSO). All rights reserved. Used with permission.

## Internal Control Components

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


*Internal Control - Integrated Framework,* ©2013 Committee of Sponsoring Organizations of the Treadway Commission (COSO). All rights reserved. Used with permission.

## Control Environment

- Set of standards, processes, and structures
- Tone at the top
- Integrity and ethical values of the political subdivision
- Includes performance measures, incentives, and rewards

Acts as the foundation for a sound system of internal control

## Risk Assessment

Risk assessment requires management to consider the impact of possible changes in the external environment and within the political subdivision that may render internal control ineffective.

- Many organizations, take a risk-based approach to internal control
- Includes:
  - Risk Identification
  - Risk Analysis
  - Risk Response

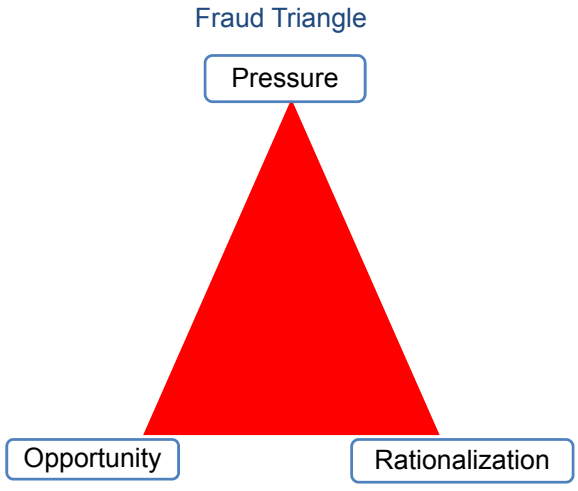
## Control Activities

Control activities are the actions established through policies and procedures to mitigate risks to the achievement of objectives.

- Preventive or detective in nature
- Manual and automated activities
- Includes segregation of duties

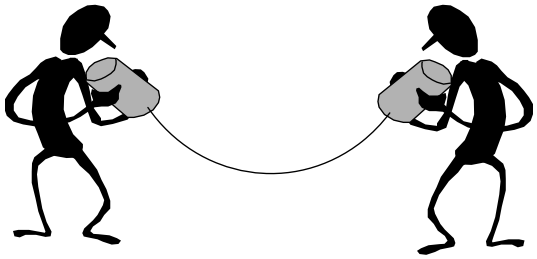
## Internal controls combat fraud and mistakes

- Prevent Opportunity
- Detect Fraud, Errors and Omissions



## Information and Communication

- Emphasizes importance of quality information
- Volume and sources
- Complexity of processes
- Technology advances
- Greater interaction with 3rd party vendors



## Monitoring Activities

| Ongoing Evaluations | Separate Evaluations |
|---|---|
| • Built into the business process at various levels<br>• Timely information | • Conducted periodically<br>• Frequency will depend on assessment of risks and effectiveness of ongoing evaluations |

## New Principles

COSO/Green Book clarifies requirements for effective internal control with the 17 new principles

- Principles relate to a component of the internal control system
- Common sense

## Control Environment

1. The oversight body and management demonstrate a commitment to integrity and ethical values.
2. The oversight body oversees the entity's internal control system.
3. Management establishes an organizational structure, assigns responsibility, and delegates authority to achieve the political subdivision's objectives.
4. Management demonstrates a commitment to attract, develop and retain competent individuals.
5. Management evaluates performance and holds individuals accountable for their internal control responsibilities.

## Risk Assessment

6. Management defines objectives clearly to enable the identification of risks and defines risk tolerances.
7. Management identifies, analyzes and responds to risk related to achieving the defined objectives.
8. Management considers the potential for fraud when identifying, analyzing and responding to risks.
9. Management identifies analyzes, and responds to significant changes that could impact the internal control system.

## Control Activities

10. Management designs control activities to achieve objectives and respond to risks.
11. Management designs the political subdivision's information system and related internal control activities to achieve objectives and respond to risks.
12. Management implements control activities through policies.

## Information and Communication

13. Management uses quality information to achieve the political subdivision's objectives.
14. Management internally communicates the necessary quality information to achieve the political subdivision's objectives.
15. Management externally communicates the necessary quality information to achieve the entity's objectives.

## Monitoring Activities

16. Management establishes and operates monitoring activities to monitor the internal control system and evaluate the results.
17. Management remediates identified internal control deficiencies on a timely basis.

## Take it Step by Step and see where it leads you!

1. Control Environment
2. Risk Assessment
3. Control Activities
4. Information and Communication
5. Monitoring

## Documentation

Start with documenting the 5 components in significant areas first.

- Cash handling
- Management's Goals
  - Customer Service
  - Compliance with Laws and Regulations

## Find where there is risk that is not mitigated by internal control

- This is Risk identification
- Perform your risk analysis
- Respond to the risk
  - Implementing controls
  - Insurance
  - Acceptance of the Risk

## Are you going to "trust" or "**make sure**" things are done right in your office?

# Examples of Internal Control Procedures

**INTRODUCTION**

Governments provide services to their citizens. Locally these services can include public safety, education, highways and streets, health and welfare, culture and recreation, economic development and public utilities. In order to fund those services, governments procure resources through taxation, fees, fines, permits/licenses, donations and grants from other governments. Governments must aim to make the most effective and efficient use of these resources in rendering services. A sound internal control system provides reasonable assurance that a political subdivision will accomplish its mission and objectives with accountability and transparency.

This section contains ideas of policies, procedures and other considerations for the development and implementation of a reliable internal control system. However, this section should not be construed as a prescribed system of internal control. The oversight body and management are responsible for developing and implementing an internal control system which meets the needs of the political subdivision.

**Component One: Control Environment**

The control environment sets the tone of the organization and influences the effectiveness of internal controls within the government. Many factors determine the control environment, including the oversight body's attitude, actions, and values; commitment to competence and human resource policies and practices; assignment of authority and responsibility; and participation.

**Principle 1. The oversight body and management demonstrate a commitment to integrity and ethical values.**

As part of its commitment to an overall system of internal control, the oversight body develops and implements a formal ethics policy. In order to ensure the policy is communicated to each person, a system of annual acknowledgment could be devised; for example, through e-mail submission or manual documentation, each official and employee attests they have read the policy and will adhere to the policy.

In furtherance of its commitment to integrity and ethical values, the oversight body and management consider the following procedures:

- Conveying periodic messages of philosophy and expectations to all employees.

# Examples of Internal Control Procedures

- Evaluating the internal control system for weaknesses on a regular basis, providing resolutions to any weaknesses, and informing employees of changes in procedure.

- Establishing a confidential reporting system for individuals to report suspected fraud and abuse of local policies.

- Instituting procedures to address violations of policies and consequences for violation.

**Principle 2. The oversight body oversees the entity's internal control system.**

If considered necessary, the legislative body establishes an oversight committee and appoints members with high ethical values, excellent communication and problem solving skills. This committee oversees the internal control system and advises the legislative body and management on internal control issues. In the event that an oversight body is not created, the legislative body would be responsible for overseeing the internal control system for the entity.

Management provides documented control processes to the oversight body for review and input. The oversight body should analyze the internal control system for weakness on an entity-wide basis as well as on a departmental basis. Ideally, offices and departments utilize the oversight body as a resource for ideas.

To ensure inclusion of all components in the internal control system, the oversight body provides a template of the five components with corresponding principles to each person responsible for the achievement of a defined objective. The point person for a particular objective shows modifications for those areas that are directly related to the objective.

**Principle 3. Management establishes an organizational structure, assigns responsibility, and delegates authority to achieve the entity's objectives.**

Management establishes and documents the organizational structure of each office and department. Examples of items to incorporate into the structure include:

- An organizational chart.

# Examples of Internal Control Procedures

- An outline of specific duties within the organizational structure.
- Designation of responsible persons for each part of the accounting process.
- Documentation of internal control procedures over specific accounting areas, including communication and monitoring.
- Correlation of assigned responsibility and authority to entity objectives.

**Principle 4. Management demonstrates a commitment to recruit, develop, and retain competent individuals.**

Management determines the skills necessary for each level of the organizational chart and assesses each employee for skills necessary to accomplish the assigned responsibilities. The oversight body develops a plan to continually train employees on new procedures, laws, and governmental guidelines. Items to consider include:

- Creating job descriptions and determining skills necessary to perform jobs.
- Tracking the training schedules and review courses for each employee.
- Completing evaluations on a regular basis and addressing any deficiency in skills.
- Assessing the best recruitment pools for the differing skill sets of skills, i.e., interviewing at job fairs, colleges, internship programs, etc.

**Principle 5. Management evaluates performance and holds individuals accountable for their internal control responsibilities.**

Management develops a formal employee evaluation system to assess the performance of each employee's internal control responsibilities.

The oversight body establishes overall policies with objectives that cross over offices and departments. Examples might be grant coordination, claims processing, and personnel and payroll procedures.

# Examples of Internal Control Procedures

Management establishes communication procedures to ascertain weaknesses in internal controls as well as non-compliance with internal control procedures. For example, communications may be received internally from other employees or externally from citizen complaints or issues. Procedures may include a mechanism for responding to these communications, including communication back to the employee who was non-compliant with procedures.

Management and the oversight body work together to address noncompliance with internal control procedures and take appropriate action to correct the noncompliance.

**Component Two: Risk Assessment**

Risk assessment is the process used to identify, analyze, and manage potential risks to the governmental entity's objective. When performing a risk assessment, management considers the effects of change and inherent risk.

During times of change, events can occur that expose the government to increased risk, such as change in management or responsibilities of management; rapid growth; new technology or information systems; or new programs or services. Certain activities have a greater potential for loss from fraud, waste, unauthorized use, or misappropriation. For example, the handling of cash has a much higher inherent risk for theft than data entry activities. When evaluating inherent risk, some items to consider include:

- The complexity of the activity itself or the calculations for the activity.
- The susceptibility of the activity to fraud or misappropriations.
- The extent of judgment involved for the activity.
- The size and volume of individual items comprising the activity.

Once identified, risks should be analyzed for likelihood and impact. Many risks are accepted or avoided by implementing effective controls.

# Examples of Internal Control Procedures

**Principle 6. Management defines objectives clearly to enable the identification of risks and risk tolerances.**

Objectives fall within three major categories:

Operations - Effectiveness and efficiency of operations.

Reporting – Reliability of reporting for internal and external use.

Compliance – Compliance with applicable laws and regulations.

As a part of this process, the oversight body may consider the following:

- Defining objectives in specific measurable terms in order to enable the design of internal control for related risks, to increase understanding at all levels, and to assess performance.
- Identifying what is to be achieved, who is to achieve it, how it will be achieved, and when it will be achieved.
- Incorporating external requirements, such as state statutes and Uniform Compliance Guidelines.
- Including a subset for the three categories which addresses the safeguarding of assets.

**Principle 7. Management identifies, analyzes, and responds to risks related to achieving the defined objectives.**

In the identification process, management recognizes the various types of risks at the entity and transaction levels for each objective. For example, risk factors may include the organizational structure, new technology, complexity of a program or transaction, new or amended laws, or economic instability.

Management analyzes identified risk to estimate the effect of the risk on achieving the defined objectives at the entity level and transaction level. For example,

- How likely is the risk to occur?

## Examples of Internal Control Procedures

- How will it impact the objective?
- Is the risk based on complex or unusual transactions?
- Is the risk based on fraud?

Risks may be analyzed individually or collectively. Once the risks have been identified and analyzed, management determines how to respond to each risk and design specific actions accordingly. For example, management may accept the risk and take no action in response; choose to eliminate certain processes to avoid the risk; reduce the risk by instituting controls; or transfer the risk. Certain responses to fraud risk are required by statute, such as the purchase of official bonds.

**Principle 8. Management considers the potential for fraud when identifying, analyzing, and responding to risks.**

Management considers the types of fraud which can occur, such as fraudulent financial reporting, misappropriation of assets, and illegal acts. In addition to fraud, management assesses the likelihood of other types of misconduct such as waste or abuse. Various risk factors may need to be evaluated as well as allegations from internal or external parties.

The analysis and response to fraud risk is similar to the procedures set for in the analysis and response to risk in Principle 7. Certain responses to discovered fraud are required by statute:

- IC 5-11-1-27(l) Report of Misappropriation of Funds to State Board of Accounts and Prosecuting Attorney.
- IC 5-11-1-27(j) Report of Material Variances, Losses, Shortages, or Thefts to the State Board of Accounts.

**Principle 9. Management identifies, analyzes, and responds to significant changes that could impact the internal control system.**

Internal control procedures require evaluation and adjustment on a regular basis to accommodate the impact of future changes; for example, personnel changes, newly elected officials, new programs, new technology, new laws, and financial fluctuations. For example,

# Examples of Internal Control Procedures

- New employees receive training on internal controls and employee policies.
- New software requires a reevaluation of policies and procedures to determine if existing controls will continue to be effective and if new controls need to be designed and implemented. (Procedures that worked well under a manual or a previous software system may no longer be applicable under the new system).
- A change in reporting requires a review of internal controls over the compilation of the report.

**Component Three: Control Activities**

Once risks are identified and assessed, management develops control activities to minimize the risks. Control activities detect, prevent, or reduce the identified risks that interfere with the achievement of objectives. Detection activities are designed to identify unfavorable events in a timely manner whereas prevention activities are designed to deter the occurrence of an unfavorable event. Examples of these activities include reconciliations, authorizations, approval processes, performance reviews, and verification processes.

An integral part of the control activity component is segregation of duties. However, in very small governmental units, such segregation may not be practical. In this case, compensating activities should be implemented which may include additional levels of review for key operational processes, random and/or periodic review of selected transactions. In smaller units, these reviews and testing of processes might be performed by governing boards or other elected officials.

**Principle 10. Management designs control activities to achieve objectives and respond to risks.**

Management tailors control activities to the functions of the political subdivision and documents the required procedures. The following examples of control activities are categorized by transaction type; the list is not all inclusive and would not necessarily comprise a complete internal control system.

# Examples of Internal Control Procedures

## A. Payroll Activities

1. Salaries and wage rates are verified by someone outside of the payroll process.

2. The responsibilities for hiring, terminating, and approving promotions are segregated from those preparing payroll transactions or inputting data.

3. The responsibilities for approving time sheets are segregated from those for preparing payroll transactions or inputting data.

4. Payroll adjustment reports are reviewed by someone outside of the payroll process.

5. Employees' time and attendance records are approved by their supervisors.

6. Corrections to recorded time and attendance records are approved by the employee's supervisor and authorized by management.

7. Procedures are in place to ensure that changes in employment status are promptly reported to the payroll processing unit.

8. Payroll disbursements are reviewed and approved by an authorized individual prior to payment.

9. Access to payroll applications is appropriately controlled by user logins and passwords.

10. Changes to a payroll disbursement are approved by an individual other than the ones authorized to make the changes.

11. Payroll checks are accounted for in numerical order and reconciled to the payroll check register.

12. Access to the signature stamp used to sign payroll checks is adequately controlled.

13. Payroll checks/stubs are periodically distributed by someone outside the normal payroll distribution function.

# Examples of Internal Control Procedures

14. Unclaimed payroll checks/stubs are returned to an individual other than those involved with the payroll process.

15. Employees are cross-trained on the payroll process; those assigned to payroll take mandatory vacations.

**B. Disbursement Activities**

1. The responsibility for approving claims is segregated from those preparing the claims.

2. Checks are written by an individual other than the one approving the claim.

3. Checks are signed by an individual other than the one preparing them.

4. Claims for payment are reviewed and approved by the governing body prior to payment.

5. A reconcilement is completed between the claims for payment approved by the board and the actual disbursements posted to the ledger.

6. The responsibility for acknowledging the receipt of goods or services is segregated from those preparing claims and writing checks.

7. Vendor checks are accounted for in numerical order and reconciled to the disbursement ledger.

8. Invoices or other receipts are attached to each claim to support the disbursement.

9. A review is completed by an individual outside the disbursement process in which the claim amount is compared to the supporting documentation attached to the claim and the amount of the check.

10. Access to disbursement applications is appropriately controlled by user logins and passwords.

# Examples of Internal Control Procedures

**C. Receipting Activities**

1. The responsibility for collecting money and issuing receipts is segregated from those preparing the bank deposit.

2. The responsibility for making bank deposits is segregated from those preparing the monthly bank reconcilement.

3. Pre-numbered receipts are issued for all money collected and the duplicate receipt is retained.

4. Receipts are reconciled to the cash receipts ledger by an individual other than the one collecting money and issuing receipts.

5. Posting of receipts to the ledger is completed by an individual other than the one who collects money and makes the deposit.

6. Receipts indicate the type of payment received (cash, check, etc.) and this is reconciled to the make-up of the bank deposit.

7. Accounts receivable records are maintained by an individual other than the one(s) involved in the billing process.

8. The billing process is completed by an individual other than the one who collects cash payments from customers.

9. Adjustments to customer accounts are approved by the governing body only after a thorough review.

10. A periodic review is completed of all adjustments made to customer accounts by an individual independent of the billing and accounts receivable processes to ensure that all adjustments made have proper approval from the governing body.

**D. Cash Activities**

1. A reconcilement between the recorded cash balance and the bank balance is completed monthly by an individual separate from the receipting and disbursing processes.

# Examples of Internal Control Procedures

2. A reconcilement between the receipts ledger and the credits to the bank account is completed periodically by an individual separate of the receipting process.

3. A reconcilement between the disbursement ledger and the debits to the bank account is completed periodically by an individual separate of the disbursement process.

4. The monthly reconcilement between the cash balance and the bank balance is thoroughly reviewed and approved by the governing body.

5. Disbursements from and reimbursements to petty cash funds are periodically reviewed by an individual other than the one responsible for maintaining the petty cash fund.

**E. Credit Cards Transactions**

1. A designated official or employee oversees the issuance and use of the credit cards.

2. An ordinance or resolution specifically states the purposes for which the credit card may be used.

3. The designated official or employee collects the credit card when the purpose for which the credit card has been issued has been accomplished.

4. The designated responsible official or employee maintains an accounting system or log which includes the names of individuals requesting usage of the cards, their position, estimated amounts to be charged, fund and account numbers to be charged, date the card is issued and returned, sufficient documentation provided, etc.

5. A designated person separate from disbursement process reviews transactions listed on the credit card statements for sufficient documentation and inclusion in claim to the Board.

# Examples of Internal Control Procedures

**Principle 11. Management designs the political subdivision's information system and related control activities to achieve objectives and respond to risks.**

Management may utilize Information technology (IT) systems as an integral part of the internal control system. In many cases, IT systems are used to record all financial information for a governmental entity. In these instances, the IT system may provide many different internal controls over the financial reporting process. For example:

- Permissions can be set that allow only certain users to perform certain tasks.

- Segregation of duties can occur by forcing duties to be completed by different users. For example, the system could be set to only allow User A the ability to generate receipts when money is received and only allow User B to post the receipts generated to the ledger. User B could check the receipts issued against the bank deposit to ensure that all receipts collected were deposited. Then, User B could post all the receipts to the ledger.

- The automation of processes and calculations enhances the internal control system by preventing errors. For example, posting receipt and disbursement amounts to the ledger and calculating fund balances and total receipts and disbursements may be completed automatically by the IT system. Once management verifies that the IT system has been set to ensure these procedures and calculations are completed correctly, reliance may be placed on the processes as a part of the internal control structure.

It must be noted that the use of an IT system can also create risks to the internal control structure. The procedures and calculations performed by the IT system must be checked to ensure they are functioning properly. Reliance on the IT system to perform these functions without verification of the accuracy can result in inaccurate reports and information. In addition, the IT system must also be adequately protected from

## Examples of Internal Control Procedures

unauthorized use to avoid the recording of unauthorized transactions or unauthorized changes to existing data. Also, safeguards must be established to prevent loss of data in the event of a failure of the IT system. In view of these risks, the following steps may be considered as part of the internal control system:

- Limiting the authority to access different components of the software to employees with duties specifically related to that component.
- Prohibiting User ID and password sharing between employees.
- Restricting the authority to correct or make adjustments to the records on the system to key employees or management.
- Requiring the use of prescribed forms or the approval of alternative forms.

All of these considerations, both the benefits and risks, must be weighed by the governmental entity when deciding whether or not to make the IT system a part of the internal control structure.

**Principle 12. Management implements control activities through policies.**

Management establishes policies in sufficient detail to address all identified risks. Procedures are communicated in writing to all employees that are part of the financial or reporting process. Policies set out the expectations of the oversight body and management and procedures specify the specific actions needed to comply with the policy. For example, a travel policy may require out-of-state travel to be approved in advance. The procedures outline the steps to obtain and document the approval for the claim process. In addition, management may consider the following:

- The employee handbook is provided online or in hard copy and includes internal control.
- Internal control procedures are written and available to all employees.

# Examples of Internal Control Procedures

- Variances from established procedures are brought to management's attention.
- The legislative body formalizes procedures by review and adoption during a public meeting.
- Policies and procedures are provided to other departments that are part of the financial or reporting process.
- Templates are provided for frequent procedures that document the required procedures and adherence to the procedures such as travel, credit card purchases, employee reimbursements, etc.

**Component Four: Information and Communication**

An internal control structure must provide for the identification, capture, and exchange of information within the government and with external parties. Internal communication allows supervisors to convey responsibilities and issues to their staff. In turn, staff and middle management alert upper management to potential problems; administration and program staff communicate requirements and expectations to each other. Effective communication also encourages employee involvement. In regard to external communication, management relies on the information system, including the accounting system, to accurately report activities to the Legislature, oversight agencies, and federal grantors.

**Principle 13. Management uses quality information to achieve the political subdivision's objectives.**

Information must be relevant and of high quality. The appropriate statutes, regulations, grant requirements, local ordinances, and internal reports must be the most current information available. Management determines the information needed to evaluate the internal controls established. Those needs for information are communicated to the employees so that only the most relevant and reliable information is used in the internal control procedure evaluations. The oversight body also implements policies to facilitate the flow of communication between offices or departments. The oversight body is made aware of any changes to reporting or compliance requirements that would require adjustments to the internal controls over information and communication.

# Examples of Internal Control Procedures

**Principle 14. Management internally communicates the necessary quality information to achieve the political subdivision's objectives.**

In establishing a process of internal communication, management may consider the following:

- The form of communication and documentation of internal communications between offices, departments and the oversight body is established and communicated to employees.
- Procedures are established to ensure that the communication requirements are being followed and necessary information is being communicated properly.
- Procedures are established for feedback on and clarification of the information provided.
- Internal memos and reports are maintained to document communication.

**Principle 15. Management externally communicates the necessary quality information to achieve the entity's objectives.**

In establishing a process of external communication, management may consider the following:

- Communications with State Board of Accounts, other State agencies, grantor agencies, regulatory agencies are documented by email, memos, letters and other correspondence.
- Logs are kept for information provided verbally.
- Procedures are established to retain public documents.
- Reports are cross checked for accuracy, relevancy and timeliness of information.

**Component Five: Monitoring Activities**

Monitoring activities allow management to assess the quality of internal controls over time and make adjustments as necessary. Proper monitoring ensures that controls function properly.

# Examples of Internal Control Procedures

**Principle 16. Management establishes and operates monitoring activities to monitor the internal control system and evaluate the results.**

When establishing a monitoring system, management may consider the following procedures:

- Periodic checks are performed to determine if controls are in place and working effectively.
- Control activities are reviewed to determine if the actual activities are in compliance with established procedures.
- Deficiencies in the internal control process are documented and remediation is quickly completed to address any deficiencies.

Many of the control activities can also be used as monitoring activities with the only change in the intent of the control. For example, reviewing a bank reconcilement for accuracy and supporting documents is a control activity; reviewing a bank reconciliation to ensure that appropriate personnel completed and reviewed the reconcilement in accordance with internal control procedures is a monitoring activity. Monitoring activities should be documented by signatures, initials or other methods.

**Principle 17. Management remediates identified internal control deficiencies on a timely basis.**

Internal control deficiencies may be identified internally through monitoring or externally through audit reports, communication from grantor agencies, etc. Once identified, management addresses deficiencies immediately through the development of formal or informal corrective action plans. Management and the oversight body work together to ensure the corrective action plan is implemented and the resulting changes are effective in correcting internal control weaknesses.

Management and the oversight body meet regularly to discuss controls, weaknesses and corrective action plans.

# Examples of Internal Control Procedures

**CONCLUSION**

A sound internal control system provides reasonable assurance that a political subdivision will accomplish its mission and objectives with accountability and transparency. The examples of this section provide guidance on the types of policies which could be implemented as part of an internal control system. However, the oversight body and management possess the ultimate responsibility for the design and implementation of an internal control system.

# Case Studies

## INTRODUCTION

The following case studies are taken from actual audit reports. We have included possible internal control procedures that if implemented could have helped the unit prevent or detect and correct these types of errors. The background and audit findings are real; however, the responses are suggestions only and not the required controls or the only possible controls. Each political subdivision is unique and no one response would work for each. Based on the needs of the unit, management and the oversight body will develop a unique internal control system that may include some of the suggestions as listed, or modifications of these suggestions, or internally developed controls that address the risks that management has identified. Some of the suggested controls refer to Indiana statutes and Uniform Compliance Guidelines which are required procedures. Internal controls should exist to ensure that the political subdivision is in compliance with Indiana statutes and Uniform Compliance Guidelines.

## CASE STUDY - RECEIPTING

### Background

A new Clerk of the Circuit Court was elected and no changes were made to the procedures or controls for the office. Multiple employees had access to all cash drawers in the office. The software system recorded collections to Drawer 1 and Drawer 2 and did not require identification of a specific employee with each transaction. A procedure was established where only two people, the office holder and the security administrator had access to the employees' user id's and passwords. Each employee had a unique user id and password with the exception of the 'Cash Drawer' id and password which were shared by all employees. All employees had access to all areas of the accounting system and all employees had the authorization to void transactions on the system and even the "cash drawer" user id could void a transaction. There were no established procedures to review or approve voids. Adjustments could be made to the system by all employees. There were no procedures establishing a segregation of duties in the receipting process. No paper receipts were issued for payments received and all receipting was internal to the system. There were no procedures to ensure that receipts were posted and it was assumed the bookkeeper would take care of the posting. The bookkeeper was assigned the job duties of posting, depositing and reconciling as well as being able to collect receipts.

## Case Studies

| | |
|---|---|
| Audit Results | The bookkeeper for the office was receipting cash receipts but not depositing all of the cash collections received. Because the internal controls over receipting had material weaknesses in them she was able to manipulate the records to cover her theft. In some instances, she was substituting checks to make up the for the cash collections that were misappropriated. In some cases, she would issue the receipt and then void the receipt to cover collections not deposited. Occasionally, a journal entry to adjust revenue, shown as a negative receipt, was used to cover the theft of collections. It was also discovered that the original deposit slips were altered after preparation so that the duplicate deposit slips showed a different deposit amount than what the bank received and credited to the account. Finally, source documents and revenue report for daily collections were not retained by the office and were not available for audit or for any review by the office holder.<br><br>After inspection of the bookkeeper's work computer it was discovered that she had access to every other employee's user id and password. Since cash drawers were shared among multiple employees, it was not possible to know who had actually completed the transactions. In some cases it was noted that a user id and password showed an employee making a receipt on a day that the employee was not working. Hard copy receipts were not completed so the only source documentation was the information on the computer. As a result, specific transactions could not be identified to a particular employee. Voids could be completed by any employee as there was no restriction in the rights assigned to each employee. Adjustments could be made by any employee in the system. No secondary oversight of voids or adjustments was made by anyone in the office. The bookkeeper was able to collect the payment, manipulate the system's receipting records, prepare and then alter the deposit slips, and make the bank deposit. Since she was also the person who performed the reconcilements, none of the errors or theft was detected.<br><br>Over the course of a just under three years, $75,333 was shorted from the deposits for the political subdivision. The first year, $9,042 was missing. This increased in the second year to $30,682 missing, and for nine months of the third year, prior to being discovered, $35,609 was missing. |

## Case Studies

Possible Controls:

**Component One: Control Environment**

The office holder/department head should establish an organization structure for the receipting process and provide a written copy to each employee. The structure should clearly assign each employee's duties and responsibilities. Emphasis should be made to establish the importance of ethics and integrity in completing all job responsibilities, such as:

A. The policy for the county is that all public funds are entrusted to the county and that trust should not be broken. This policy is clearly stated and communicated. (Principle1)

B. This unit is committed to integrity in providing services and an ethics policy has been written and provided to each employee. (Principle 1)

C. Internal Controls over receipting including all five components have been reviewed by the oversight body and approved. (Principle 2)

D. An organizational chart is compiled and individual job duties are outlined. (Principle 3)

E. If an employee has greater access than is needed to complete their assigned duties, that access is restricted. Cross training is completed to make sure that more than one employee is knowledgeable about the receipting process. This cross training would allow more than one employee to be aware of potential design deficiencies in the internal controls or of noncompliance with internal controls. Each employee should be encouraged to report these situations to management or the oversight body. (Principle 4)

F. Evaluations include a focus on adherence to established control procedures and skills are assessed against the employee's job responsibilities. Any additional tasks assumed by the employee are questioned. Violations are noted and corrective action is taken. Additional training is completed as necessary. All evaluations include a discussion of the internal controls and any problems the employee has with their own or another employees tasks related to internal controls.

## Case Studies

Corrective action is taken whenever necessary. Internal controls are modified as needed. Control deficiencies are communicated to the oversight body along with the corrective action plan. (Principle 5)

**Component Two: Risk Assessment**

The objectives are that all collections should be properly receipted, and timely deposited to safeguard the assets. In addition, proper posting is necessary to achieve accurate financial reporting. There are deposit laws and receipting requirements under the Uniform Compliance Guidelines with which the unit must comply. The following are suggested procedures:

A. The objective is for all collections to be deposited timely and intact and receipts to be properly issued. There is zero tolerance for theft and minimal tolerance for error. The financial ledgers, including the revenue ledger, must be up to date and accurate to provide management and the oversight body correct information. Laws regarding deposits must be followed and funds must be posted correctly to allow for proper use of the funds in compliance with statute or ordinance. (Principle 6)

B. There is a risk that errors in receipting or posting might occur and not be detected and corrected or prevented from occurring. There is a risk that the funds ledger could be incorrect and fund balances not accurate. If receipts are not posted to the correct fund, revenue or cash balances would be inaccurate and the provision of services may be impaired. (Principle 7)

C. There is always a risk, especially with cash collections, that the collections may be misappropriated prior to deposit. The records could be manipulated to cover the theft of collections. Job duties, segregation of duties and review processes should be implemented to ensure that an employee is not able to steal collections and cover up the theft. (Principle 8)

D. At the time that the office holder began in this office, internal controls should have been reviewed and evaluated. Any deficiencies that are identified should be corrected. All employees should be trained on the process and internal control procedures. New employees who do not understand the receipting process would be unable to detect problems. Without training, employees may not be aware of the reason certain

## Case Studies

controls are in place such as the requirement that passwords should not be shared and no employee should have another employee's password. Changes in software or whenever there is a change in department head or other employee means that the office or department is at a heightened risk of control systems not being followed. (Principle 9)

**Component Three: Control Activities**

Management should establish control activities that minimize the risks identified, such as:

A. Only one employee is assigned to each drawer. The employee is responsible for balancing their drawer. No other employee is authorized to use that drawer. (Principle 10)

B. Each employee will have a user id and password, these will not be shared. (Principle 10 & 11)

C. One employee will check the reconcilement of the cash drawer collections and cash change to the revenue report for that employee. (Principle 10)

D. The IT department will be consulted so that each employee is restricted in access within the software system to those areas needed to complete assigned duties only. (Principle 10 & 11)

E. All transactions will carry the unique user id of the employee that completed the transaction. (Principle 10 & 11)

F. Only the security administrator for the office/department will have access to user id's and passwords. The security administrator does not collect receipts. (Principle 10 & 11)

G. Voided transactions require second party review and authorization. A review of all voided transactions is completed by the office holder. (Principle 10)

H. Adjustments to the revenue ledger require second party review and authorization. All adjustments are reviewed by the office holder. (Principle 10)

## Case Studies

I. One employee will prepare the bank deposit. A second employee will recheck the accuracy of the deposit and a third employee will make the deposit at the bank. Duplicate receipts are returned to the employee who performs the reconcilement. (Principle 10)

J. All revenue reports will be initialed by the employee and the second party reviewer and compared to the total revenue report for the day. All reports will be maintained in a daily file. (Principle 10)

K. The office holder/department head will obtain the bank statement and review. One employee will prepare the monthly reconcilement between the bank statement and the monthly revenue report. All deposits will be traced from the bank statement back to the duplicate deposits. Any variances will be noted for immediate review. (Principle 10)

L. Receipting procedures are documented in writing and available to all employees in the office or department. Employees are encouraged to report problems they perceive in the implementation of internal controls. (Principle 12)

**Component Four: Information and Communication**

Both the oversight body and management foster an environment of open communication and feedback on the internal control system strengths and weaknesses as well as any deviations. For example,

A. Reconcilement of receipts to bank is completed and any corrections noted are posted to the revenue ledger and funds ledger prior to month end reports being prepared. (Principle 13)

B. All variances are researched and resolved and proper documentation is maintained. (Principle 13)

C. Reports are checked for accuracy and that corrections have been made for any errors detected. (Principle 13)

D. Management and the Oversight Body reviewed the controls over receipting and month end reports for reasonableness. Management and Oversight body respond to any complaints from employees or citizens on the receipting process. (Principle 14)

## Case Studies

E. Any modifications to the receipting procedures are immediately communicated to the staff. A change in job duties may be implemented for any part of the receipting process that have been determined to have a problem. (Principle 14)

F. All control deficiencies identified in an external audit are immediately addressed, evaluated and a corrective action plan is written. Management and the oversight body will follow up on the correction plan to ensure that it has been implemented and has correctly addressed the weaknesses. (Principle 15)

**Component Five: Monitoring Activities**

Office holder/department head should spot check bank reconcilements, cash drawer counts, receipts for the month throughout the month. Clearly identify if controls are being used as designed and look for any noncompliance with established procedures:

A. Office holder/department head reviews completed bank reconcilements each month and initial off that the reconcilement has been checked. (Principle 16)

B. Revenue reports generated from the months receipts are sent to the department head/office holder for review for accuracy and reasonableness. Monthly revenue is compared to prior months and same month from a year ago to determine reasonableness. (Principle 16)

C. Any violations of policies and procedures will be noted and evaluated. Internal Controls may be reevaluated to correct the problems discovered. (Principle 17)

### CASE STUDY – RECEIPTING (Small Unit)

Background

The town used a computer software system to record billings and collections of utility services provided to its citizens. The setup of the computer system authorized the Clerk-Treasurer and two other employees to make entries to the individual citizen accounts. According to the Clerk-Treasurer, at the end of each day the Utility Clerk or the

## Case Studies

Deputy Clerk-Treasurer was responsible for running the End of Day Report, totaling the payment stubs, and balancing the cash drawer. She would then complete the bank deposit ticket, and finally take the deposit to the bank. For days in which the Utility Clerk performed the End of Day duties, the Deputy Clerk-Treasurer was supposed to verify that the End of Day report, adding machine tape, cash drawer, and deposit agreed and vice versa. Each Clerk was supposed to initial off on the supporting documentation to indicate that the verification had been completed. The computer software system required each user to have a user id and password. Each payment that was posted indicated a Clerk that supposedly made the entry. The payment posting would automatically be recorded in the Customer Account history portion of the system, which the town employees were not aware of.

The town used a manual system for collecting and recording utility meter deposits. When a new customer requested utility services, they were required by a town ordinance to complete an application and pay a specific meter deposit amount. According to the Clerk-Treasurer, all employees were authorized to accept applications and payments. When the town employee was presented with an application, they calculated the meter deposit, accepted payment, and completed a two-part hand written receipt. The first copy of the receipt was given to the customer and the second part was retained in the receipt book. The employee was also required to note on the application the payment amount, date, and receipt number. The payment was entered into the town's financial computer system that would create a receipt to document posting to the appropriate fund. The employee responsible for accounting for the day's collections used the computer generated receipts to compile the bank deposit. The town also maintained a manual "Guarantee Deposit Register" where they would record meter deposits collected, released/refunded, and held.

Audit Results

We found the End of Day and verification procedures were not performed consistently enough to be effective. However, when we compared the user id noted on various reports to time cards for each clerk we found instances in which the person's user id noted was not actually working on that particular day. We concluded that the town employees were not maintaining confidentiality of their username and passwords. We found that the employees were not aware that the

## Case Studies

payments they entered were recorded on the Customer History reports. We traced payments posted from the Customer History reports to the actual bank deposits and found $47,057.31 in posted payments that were not deposited in the Town's bank account.

We found that $3,300.00 of hand-written receipts and postings to the "Guarantee Deposit Register" were not deposited in the Town's bank account.

Possible Controls:

**Component One: Control Environment**

A. The elected officials (Town Council and Clerk-Treasurer) could clearly express the expectations they have for all employees to conduct themselves and complete their duties with integrity. (Principle 1)

B. It appeared that the Clerk-Treasurer had assigned duties, but could have made them more specific and stressed the importance of the tasks being segregated. (Principle 3)

C. The Town Council could have reviewed the duties assigned by the Clerk-Treasurer and periodically meet with her to evaluate the office procedures and the employees that are completing those tasks. (Principle 2)

D. The Clerk-Treasurer could have required that each employee that accepted payments have their own cash drawer. (Principle 3)

E. She could have relayed the importance of each employee not sharing their usernames and passwords. She could have understood the computer accounting system and used any built-in security measures to establish and evaluate procedures. (Principle 3)

F. The Clerk-Treasurer and the Town Council could develop education and experience guidelines to use during the hiring process in order to guide them in employing competent individuals. (Principle 4)

## Case Studies

G. The Clerk-Treasurer could establish an annual employee evaluation process to determine areas in which the town employees are excelling and areas in which they need additional training. (Principle 4)

H. Town Council could support the evaluation system by indicating it would be relied upon in determining additional benefits and disciplinary measures for the future. (Principle 4 and 5)

**Component Two: Risk Assessment**

A. After the Clerk-Treasurer assigns the specific duties in the receipt process, she could determine the likelihood that an employee would make an error or misappropriate funds while completing their duty. (Principle 6)

B. She could have consulted with the Town Council to identify the risky areas and they could determine the mitigating procedures that they would institute to lessen the risk of theft or error. (Principle 7)

C. The risks could include an employee manipulating the computer system resulting in theft (Principle 8). Receipts not posted correctly or not posted at all could create financial reports that don't give an accurate account of the fund activities and balances, therefore proper decisions may not be made. (Principle 8)

D. The Clerk-Treasurer and Town Council could develop contingency plans for situations in which the make-up and environment of the Town changes significantly. For example, if the Utility Clerk position is vacant for a number of months, then the Clerk-Treasurer could establish some additional mitigating controls involving the Town Council to ensure the internal control system continues to function. (Principle 9)

**Component Three: Control Activities**

As much as possible the procedures to collect, verify, deposit, and post payments need to be segregated among all employees of the Town. Any reviews performed could be documented by the reviewer initialing the receipt/report/deposit being verified.

A. The Clerk-Treasurer with approval of the Town Council could formalize the procedures below by officially adopting similar procedures as below. (Principle 12)

## Case Studies

B. The Utility Clerk could be responsible for collecting payments from customers and issuing receipts. The Utility Clerk counts the drawer to determine total amount collected for the day. (Principles 10 & 11)

C. The Deputy Clerk-Treasurer reconciles the End of Day Collections report to the cash drawer and completes the deposit ticket. She could also make any corrections/adjustments requested to customer accounts. (Principles 10 & 11)

D. The Clerk-Treasurer reviews the receipt postings to the customer accounts, verifies the deposit to the deposit ticket and makes the deposit at the bank. She could also review all adjustments to customer accounts. (Principles 10 & 11)

E. The computer accounting system will restrict users from performing tasks that they are not assigned. The system could limit the ability of certain users to record voids or adjustments to individual's accounts. The system could date and time stamp reports used to reconcile collections to deposits. (Principles 10 & 11)

F. The Town Council could review reports that compared billings to collections that could indicate if unexpected postings were being made. They could also compare collection reports to bank statement deposits to assess if collections are being deposited. (Principles 10 & 11)

**Component Four: Information and Communication**

A. The Clerk-Treasurer could document and share with the employees and Town Council the tasks that are assigned to each employee. (Principle 14)

B. She could encourage everyone to evaluate the procedures that she assigns and provide information that could make the internal controls more effective. (Principle 14)

C. She could determine the supporting documents and reports that are needed to provide an evaluation that the payments received have been posted and deposited. (Principle 13)

D. The Town Council could inquire/ensure that all employees are performing their assigned tasks. The Clerk-Treasurer could provide notification, through signage, that all customers making a payment would receive a receipt and customer payment histories would be available upon request. (Principle 15)

## Case Studies

| | |
|---|---|
| **Component Five: Monitoring** | A. The Clerk-Treasurer could do random checks of a day's cash collections to what was counted by the Utility Clerk and verified by the Deputy-Clerk Treasurer. (Principle 16)<br><br>B. She could look for areas in which the internal control procedures were not followed. (Principle 17)<br><br>C. The Town Council could randomly request to review collection reports and bank reconcilements to determine if the information that they are being provided is reliable. (Principle 16)<br><br>D. The Clerk-Treasurer and the Town Council could periodically meet to evaluate the internal control procedures that have been put in place to determine if they need to be updated for controls that are ineffective. (Principle 17) |

**CASE STUDY – CREDIT CARDS**

| | |
|---|---|
| Background | The fiscal officer of a political subdivision used numerous credit cards issued in the name of the political subdivision for unauthorized personal purchases in the amount of $346,156. The purchases, which spanned a period of six years, included personal items such as food, alcohol, gift cards, toys, grocery, clothing, jewelry, sales tax, batteries, and other miscellaneous merchandise. |
| Audit Results | 1. The political subdivision did not have a formal policy governing the use of credit cards.<br><br>2. Payments were not supported by a claim and were not approved by the legislative body.<br><br>3. Credit card purchases were not supported by documentation, such as receipts or invoices.<br><br>4. Incompatible activities related to disbursements were not separated. |

# Case Studies

Possible Controls

**Component One: Control Environment**

The oversight body and management set the tone of the organization, which directly influences the effectiveness of internal controls within the government. In this case, the political subdivision did not have a formal policy governing the use of credit cards. Suggested procedures related to credit card usage:

A. The oversight body and management demonstrate a commitment to integrity and ethical values by stressing adherence to statutory provisions regarding the payment of claims, the prescribed accounting system, and uniform compliance guidelines published by the State Board of Accounts. (Principle 1)

B. The oversight body adopts a credit card policy with the minimum requirements set forth in the State Board of Accounts uniform compliance guidelines. (Principle 2)

C. Management emphasizes organizational structure and specifically assigns responsibilities not otherwise delegated by statute, for example individuals responsible for maintaining custody of the cards, reviewing claims for sufficient documentation, and reconciling the credit card statement to approved claims. (Principle 3)

D. Employees involved in the credit card process are trained and educated on proper usage, accountability, adherence to the credit card policies, and compliance with state statutes. (Principle 4)

E. During the claim approval process, the oversight body and management evaluate the credit card claims for adherence to the policy. In the Credit Card Policy, management considers the consequences for failure to follow required procedures; for example, the consequences and responsibility for late charges, insufficient documentation, or personal use. (Principle 5)

## Case Studies

**Component Two: Risk Assessment**

Management should define objectives to identify risks and then develop procedures to mitigate the risk. In this case, management had no policies or procedures in place to limit the use of the credit cards, detect fraud, or reduce non-fraud risk associated with credit card usage. If management had defined objectives and identified risks, they would have developed controls to mitigate those risks. Suggested procedures include the following:

A. Example objectives

**Operations Objective:** All credit card charges must be for a business purpose, be supported by appropriate documentation, and submitted in a timely manner.

In order to accomplish this objective, management defines acceptable business uses, supporting documentation, and timely submission and designates a person responsible for ensuring compliance with the policy. Ideally this person does not have credit card purchasing authority.

**Reporting Objective:** All credit card charges must be accurately reported in the financial statements.

In order to accomplish this objective, management requires a procedure comparing bank statement disbursements to approved claims.

**Compliance Objective:** Credit card claims must meet the requirements of IC 5-11-10 and be on a form prescribed by the State Board of Accounts.

In order to accomplish this objective, management reviews claims individually for supporting documentation, rather than just signing the Accounts Payable Voucher. (Principle 6)

B. Management identifies risk, analyzes risk, and develops procedures to mitigate risks associated with credit card usage. Examples of risk, other than fraud risk, are as follows:

- Non-compliance with statutes.
- Insufficient Documentation.

## Case Studies

- Interest and Finance Charges.
- Unnecessary expenses.
- Insufficient appropriation.
- Lost or stolen cards.
- Noncompliance with other policies or ordinances. (Principle 7)

C. Management mitigates risk through the adoption of the Uniform Compliance Guidelines related to credit cards, as follows:

1. The governing board must authorize credit card use through an ordinance or resolution, which has been approved in the minutes.

2. Issuance and use should be handled by an official or employee designated by the board.

3. The purposes for which the credit card may be used must be specifically stated in the ordinance or resolution.

4. When the purpose for which the credit card has been issued has been accomplished, the card should be returned to the custody of the responsible person.

5. The designated responsible official or employee should maintain an accounting system or log which would include the names of individuals requesting usage of the cards, their position, estimated amounts to be charged, fund and account numbers to be charged, date the card is issued and returned, etc.

6. Credit cards should not be used to bypass the accounting system. One reason that purchase orders are issued is to provide the fiscal officer with the means to encumber and track appropriations to provide the governing board and other officials with timely and accurate accounting information and monitoring of the accounting system.

## Case Studies

7. Payment should not be made on the basis of the statement or a credit card slip only. Procedures for payments should be no different than for any other claim. Supporting documents such as paid bills and receipts must be available. Additionally, any interest or penalty incurred due to the late filing or furnishing of documentation by an officer or employee should be the responsibility of that officer or employee. (Principle 7)

D. Management considers the types of fraud which can occur with credit card usage, including, but not limited to fraudulent financial reporting and misappropriation of assets. In addition to fraud, management weighs the likelihood of other types of misconduct such as waste or abuse. Considerations which may reduce the potential for fraud include the following:

1. The number of cards needed. In this case, an extraordinarily large number of credit cards were issued to the unit.

2. Designation of authorized users; documentation that authorized users have agreed to the terms of the credit card policy, statutory provisions, and the prescribed accounting system.

3. Written direction on the purposes or circumstances for which the cards may be used, including appropriate purchases and/or appropriate vendors.

4. Restrictions placed on the cards to reduce or mitigate the risks, such as a reasonable credit limit, deactivation of cash advancement features, limitation on the purchase amount per transaction, etc. (Principle 8)

E. In responding to risk, management reviews the official duties of all employees and purchase adequate bond coverage at amounts equal to or above the minimum amount required by statute.

In response to fraud or variances, management must comply with certain reporting statutes:

- IC 5-11-1-27(l) Report of Misappropriation of Funds to State Board of Accounts and Prosecuting Attorney.

## Case Studies

- IC 5-11-1-27(j) Report of Material Variances, Losses, Shortages, or Thefts to the State Board of Accounts. (Principle 8)

F. The internal controls and policies related to credit card usage must be evaluated and adjusted on a regular basis for personnel changes, newly elected officials, financial fluctuations, etc. (Principle 9)

**Component Three: Control Activities**

In this case, control activities were not sufficient to detect fraudulent use of credit cards; incompatible activities were not separated. In addition to the policies and procedures outlined in the Control Environment and Risk Assessment section, management may consider the following suggested procedures.

A. Management assigns a person, other than the official custodian of the credit cards or fiscal officer, to match invoices to charges on the credit card statements and analyze the use of the credit card against adopted policy. In this case, the designee would have noticed that certain charges were not supported by invoices or not related to a business purpose. (Principle 10)

B. Management assigns a person, other than the official custodian of the credit cards or fiscal officer, to reconcile the credit card statement to credit card claims approved by the legislative body. In this case, the designee would have noticed that the total dollar amount paid on the credit card statement was more than the claim approved by the legislative body. (Principle 10)

C. Management assigns a person the responsibility to reconcile disbursements per the bank statement to approved claims. In this case, the designee would have noticed that the total dollar disbursements to credit card vendors were more than the claims approved by the legislative body. (Principle 10)

**Component Four: Information and Communication**

Management should receive quality information from internal and external sources regarding credit card usage. If management had reviewed credit card statements and bank statements along with the claims presented for approval, they would have been able to detect additional charges not submitted for approval. (Principle 13)

## Case Studies

| | |
|---|---|
| **Component Five: Monitoring** | A designated person, such as an office holder or department head, periodically reviews the completion of designated policies and procedures, such as control activities and determines if controls are being used as designed. Suggested monitoring procedures include:<br><br>A. An office holder or department head periodically reviews the analysis of sufficient documentation and appropriate expenses for credit card transactions. (Principle 16)<br><br>B. An office holder or department head periodically reviews the reconciliation of the credit card statement to the approved claims related to credit card transactions. (Principle 16)<br><br>C. An office holder or department head periodically reviews the reconciliation of bank statement disbursement to approved claims. (Principle 16)<br><br>D. Violations of policies and procedures are noted and evaluated. (Principle 17) |
| **CONCLUSION** | In this case, the governmental unit lacked policies and procedures related to the five components and seventeen principles of internal control. An effective system of internal control could have detected the fraud sooner, resulting in a much smaller loss to the taxpayers. |

# APPENDIX

## INTERNAL CONTROL TRAINING CERTIFICATION FOR ELECTED OFFICIALS, APPOINTEES, AND EMPLOYEES

I, _____, the duly elected, appointed, or employed
(print name)

_____ for _____ certify that I
(position or title) (political subdivision)

received the following training concerning internal controls standards and procedures as required by Ind. Code § 5-11-1-27(g)(2):

| Title of Training | Time Spent |
|---|---|
| _____ | _____ |
| _____ | _____ |
| _____ | _____ |

Date: _____ _____
Signature

* This certification may be printed, signed, and retained in paper form or electronically. If signed electronically, the elected official, appointee, or employee must designate his or her signature by typing the last four (4) digits of their Social Security number in the signature line.