



Uniform Compliance Guidelines on Internal Controls for State and Quasi Agencies

Paul D. Joyce, CPA
State Examiner

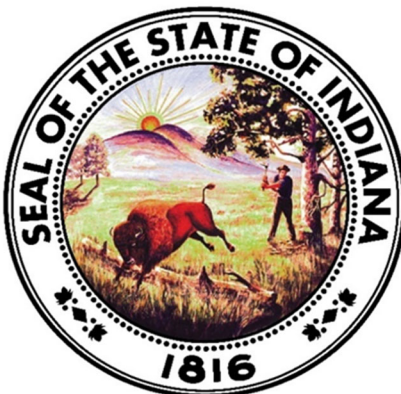


Table of Contents

Introduction

Overview	7-9
Uniform Compliance Guidelines	7
Five Components of Internal Control.....	7-8
Definition of Internal Control.....	8-9
Cost Benefit of Internal Controls.....	9
Why It Matters	9-10
Where to Start	10-11
Documentation of the Internal Control Plan	11-12

Part One: The Internal Control Guidelines

Overview	15
Description of Internal Control Guidelines	16
Control Environment.....	17-20
Risk Assessment	20-23
Control Activities.....	23-26
Information and Communication.....	26-28
Monitoring	29-30

Part Two: Evaluation and Development of the Agency Internal Control System

Section One: Control Environment

Overview	33
Why It Matters	33
Where to Start	34-35

Table of Contents

Developing the Control Environment	35-39
Set the Tone at the Top	36
Define and Communicate Standards of Conduct.....	36-37
Evaluate Adherence to Standards of Conduct	37
Establish Oversight Structure and Procedures	
for the Internal Control System	37
Design Agency Organizational Structure.....	38
Recruit, Develop, and Retain Competent Staff	38
Create Succession and Contingency Plans	39
Promote Accountability	39
Documenting the Agency Control Environment	39-40
Section Two: Risk Assessment	
Overview	43
Why It Matters	43
Where to Start	44
Conducting a Risk Assessment	45-52
Define the Agency’s Mission Statement and Related Objectives	45-47
Identify Risks to the Achievement of Objectives	47-48
Prioritize Identified Risks.....	48-49
Respond to the Identified Risks	49-50
Consider the Potential for Fraud.....	50-51
Identify and Assess Risk from Change	52
Documenting the Risk Assessment Process.....	53

Table of Contents

Section Three: Control Activities

Overview	57
Why It Matters	57
Where to Start	57-58
Developing Agency Control Activities	58-68
Respond to Risks	60
Design Control Activities	61-65
Specifically Address the Information System	65-67
Document Control Activities	67
Communicate Responsibility.....	67
Review Policies and Procedures.....	68
Documenting Control Activities	68

Section Four: Information and Communication

Overview	71
Why It Matters	71-72
Where to Start	72-73
Developing Agency Information and Communication Processes	73-77
Identify Information Requirements	74
Gather Quality Data	75
Process the Information.....	75
Establish Internal Communication Pathways.....	75-76
Establish External Communication Channels.....	76-77
Documenting Agency Information and Communication Processes.....	77-78

Table of Contents

Section Five: Monitoring

Overview	81
Why It Matters	82
Where to Start	82-83
Developing Agency Monitoring Procedures	84-90
Define Key Controls.....	85
Establish a Baseline.....	86
Set Benchmarks	86
Select Monitoring Methods.....	86-88
Gather Information.....	88-89
Assess Monitoring Results	89
Implement Corrective Action.....	89-90
Documenting Monitoring Procedures	90-91

Part Three: Tools for Evaluation and Development of the Agency Internal Control System

Tools for Evaluation.....	95-119
Tools for Development.....	121-122
Examples	
Examples Overview	123
Objectives, Risks, and Key Controls.....	124-154

Uniform Compliance Guidelines on Internal Controls for State and Quasi Agencies

Introduction	Issue Date: April 11, 2024
	Revision Date:

Table of Contents

Overview 7-9

Uniform Compliance Guidelines..... 7

Five Components of Internal Control 7-8

Definition of Internal Control 8-9

Cost Benefit of Internal Controls 9

Why It Matters 9-10

Where to Start 10-11

Documentation of the Internal Control Plan 11-12

Introduction

Overview

Uniform Compliance Guidelines

The head of each agency must establish, implement, and maintain an effective system of internal control in accordance with state policy and financial management circulars. To provide additional guidance for state agencies, the State Examiner compiled internal control standards in this publication: *Uniform Compliance Guidelines on Internal Controls for State and Quasi Agencies*. Based on standards advocated by leading authorities in the field of internal control, these standards are considered uniform compliance guidelines of the State Board of Accounts. The internal control process will be evaluated accordingly in any audits of State and Quasi agencies that are performed by or on behalf of the SBOA.

Five Components of Internal Control

The five components of internal control are recognized as basic to any internal control system:

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

The Committee of Sponsoring Organizations of the Treadway Commission (COSO) provides a framework that includes fundamental 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 based on these conceptual frameworks.

Because state and quasi agencies vary in size and complexity, no single method or set of internal control policies and procedures universally applies. While this manual provides minimum requirements, other publications may be beneficial for tailoring controls to an agency's specific needs. We highly recommend using the "Green Book" as a companion guide: www.gao.gov/greenbook.

Introduction

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 internal control.

Definition of Internal Control

By necessity, the definition of internal control is broad, serving as a conceptual process applied to a wide range of situations and environments. The purpose of the internal control process is to provide reasonable assurance that the mission and objectives of the state will be achieved. Namely, internal control –

- reduces risk associated with fraud and safeguards resources from loss due to waste, abuse, mismanagement, or errors.
- provides a check and balance system over operations, promoting operational effectiveness and efficiency.
- produces reliable financial and management data.
- ensures accuracy and timeliness in reporting.
- promotes compliance with laws.

SBOA defines internal control as follows:

Internal control is a process executed by officials and employees designed to provide reasonable assurance that objectives will be achieved.

- It is a basic element fundamental to the state, 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.
- It is dependent on officials and employees for effective implementation.

Each of the five components of internal control must be present and functioning to form a complete internal control process. If any of the five components is missing, true internal control is not achieved. Additionally, each component encompasses several underlying principles. To have a complete component, the principles associated with each component must be present.

Introduction

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.

Cost Benefit of Internal Controls

Because internal controls are a means to an end, they must help, rather than prevent or delay, an agency in reaching its objectives. Before designing and implementing internal controls, managers should consider the following:

- Internal controls must benefit, rather than hinder, the agency.
- Internal controls must make sense within each agency's unique operating environment.
- Internal controls must be cost effective.

Why It Matters

There are many benefits of a well-defined, relevant internal control process. Overall, Internal controls provide a process to help each agency fulfill its objectives and enhance accountability, transparency, efficiency, and effectiveness – all of which contribute to great government service.

- **Accountability.** An effective internal control system provides reasonable assurance that agencies will achieve objectives. Such objectives include, but are not limited to, utilizing public resources in compliance with laws, regulations, and budgetary limitations. An internal control system also provides reasonable assurance that financial reports are accurate, and it limits the opportunity for theft or unauthorized use of assets, including cash, inventory, and capital assets.

Introduction

- **Efficiency and Effectiveness.** Internal control procedures encourage wise use of government time and resources through the establishment of baselines and other measurable goals. Measurable goals and objectives allow agencies to gauge success in the performance of missions and objectives and adjust when necessary. Internal control processes deliver the highest value and best outcome in the completion of operational, reporting, and compliance responsibilities.
- **Sound Management Practices.** Each agency exists to accomplish its mission and related objectives. Management works with leadership to design internal controls to reasonably ensure success. Internal control processes coordinate policies and procedures to safeguard assets, check the accuracy and reliability of data, promote operational efficiency, and encourage adherence to prescribed managerial policies. Management must develop, implement, monitor, and update an effective plan of internal controls. The plan developed will depend, in part, on management's estimation and judgment of the benefits and related costs of control procedures, as well as available resources.

Where to Start

Part Two of this manual follows the five components of internal control with recommendations and tools to evaluate and develop internal controls. Within each section is an overview of the component, why it matters, where to start, and recommended steps.

What are the key risks for my agency? The first step involves identifying, analyzing, and prioritizing risk through agency risk assessments. The Risk Assessment chapter contains recommendations and optional tools for evaluating and developing the agency risk assessment process.

What controls do we have now? The agency may have controls already in place to address key risks. Management evaluates current controls, starting with key risks and audit findings. Each chapter contains recommendations and optional tools for evaluating each component based on best practices.

Introduction

Which controls need development or improvement? After prioritizing key risks and evaluating each component, management determines which controls should be developed or improved. Each chapter includes recommendations and an optional tool for the development of key internal controls for each component.

Who facilitates risk management activities? Each agency shall assign a person to the role of internal control officer as the single point of contact to facilitate and support risk management activities, including the agency risk assessment, internal control evaluation and development. The internal control officer must have the cooperation and commitment of agency leadership (agency/department/division heads) to be successful.

Documentation of the Internal Control Plan

An internal control plan is a high-level agency-wide summarization of the agency's risks and the controls designed to mitigate those risks. At a minimum, the internal control plan will address the five components of internal control for key objectives. Larger agencies may wish to develop an internal control plan for each major service area or department.

Documentation is a necessary part of effective internal control. Agency policies and procedures support the internal control plan by relating internal control procedures to the missions and objectives of the agency; solidifying expectations; and providing an effective way to communicate the process. For audit purposes, evidence must be maintained to show the performance of internal control procedures.

As a best practice, SBOA recommends the minimum documentation requirements found in the "Green Book." These Standards include minimum documentation requirements as follows:

- Management develops and maintains documentation of its internal control system.
- If management determines that a key internal control principle is not relevant, management supports that determination with documentation that includes the rationale of how, in the absence of that principle, the associated component could be designed, implemented, and operated effectively.

Introduction

- Management documents in policies the internal control responsibilities of the agency.
- Management evaluates its operations and risks and documents its assessment of vulnerabilities.
- Management evaluates and documents the results of ongoing monitoring and separate evaluations to identify internal control issues.
- Management evaluates and documents internal control issues and determines appropriate corrective actions for internal control deficiencies on a timely basis.
- Management completes and documents corrective actions to remediate internal control deficiencies on a timely basis.

Uniform Compliance Guidelines on Internal Controls for State and Quasi Agencies

Part One: Internal Control Guidelines	Issue Date: April 11, 2024
	Revision Date:

Table of Contents

Overview	15
Description of Internal Control Guidelines	16
Control Environment.....	17-20
Risk Assessment	20-23
Control Activities.....	23-26
Information and Communication.....	26-28
Monitoring	29-30

Five Components of Internal Control

Overview

A strong internal control system yields success, making it relevant to all of us. Design and implementation take time, effort, and resources in conjunction with a foundational knowledge of internal control components and principles.

The Committee of Sponsoring Organizations of the Treadway Commission (COSO) provides a framework that includes fundamental characteristics of these five components and three categories of generalized objectives. The U.S. Government Accountability Office 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." The State Board of Accounts *Uniform Compliance Guidelines on Internal Controls for State and Quasi Agencies* is organized based on these conceptual frameworks.

The five components of internal control must be successfully designed, implemented, and functioning for an effective internal control system. Seventeen principles accompany the five components, representing fundamental concepts associated with particular components within the system. All components and principles comprise an effective internal control system.

Points of focus support each principle, expressing important characteristics associated with the principles. While the components and principles are considered criteria for an effective internal control system, points of focus serve as guidance to assist management in designing, implementing, and assessing internal control. Management has latitude to determine suitability of the points of focus.

A system of internal control may be implemented in many ways. Because state and quasi agencies vary in purpose, size and complexity, no single method of internal control universally applies. However, the five internal control components and seventeen principles must 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.

Five Components of Internal Control

Description of Internal Control Guidelines

The internal control guidelines consist of the following five components:

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

Three categories of objectives focus on separate aspects of internal control.

- **Operations** – pertaining to effectiveness and efficiency of agency operations, including operational and financial performance goals, and safeguarding assets against loss.
- **Reporting** – relating to internal and external financial and non-financial reporting, encompassing reliability, timeliness, transparency, or other terms as set forth by regulators, standard setters, or agency policies.
- **Compliance** – dealing with adherence to laws and regulations.



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

Five Components of Internal Control

Control Environment

The control environment is the basic commonality for all and comprises the integrity and ethical values of the agency established by leadership. The standards, processes, and structures which form the control environment pervasively impact the overall system of internal control. Leadership conveys expectations and overall tone which are reinforced by management throughout the agency and its departments. The control environment also contains the overall accountability structure for all employees through performance and reward measures. Within this structure, management demonstrates commitment 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.

Principles one through five must be implemented and effectively working together to achieve the control environment component. Five of the seventeen principles of internal control pertain to the control environment.

Principle One:
The agency demonstrates a commitment to integrity and ethical values

Points of Focus

- **Sets the tone at the top.** Management demonstrates, through policies, actions, and behaviors, the importance of integrity and ethical values to support the functioning of the internal control system.
- **Establishes standards of conduct.** The key elements of integrity and ethical values pervade defined standards of conduct and expectations understood at all levels by employees, contractors, and stakeholders. While it is management's responsibility to establish and communicate the values of the organization, it is everyone's responsibility to demonstrate integrity. In an organizational context, ethical values are the standards of behavior that form the framework for employee conduct, guiding employees in decision making.
- **Evaluates adherence to standards of conduct.** Processes exist to evaluate the performance of individuals and teams against expected standards of conduct.
- **Addresses deviations in a timely manner.** Deviations from expected standards of conduct are identified and remedied in a timely and consistent manner.

Five Components of Internal Control

Principle Two:

Agency leadership oversees the internal control system.

Points of Focus

- **Establishes oversight responsibilities.** Leadership identifies and accepts its oversight responsibilities in relation to established requirements and expectations.
- **Applies relevant expertise.** Leadership defines, maintains, and periodically evaluates the skills and expertise of its members.
- **Operates independently.** Leadership works independently and objectively.
- **Provides oversight for the internal control system.** Leadership oversees management's design, implementation, and operation of the internal control system.

Principle Three:

Management establishes an organizational structure, assigns responsibility, and delegates authority to achieve agency objectives.

Points of Focus

- **Considers all structures of the entity.** Structure supplies the framework to carry out the agency's plans. Management considers multiple structures to support the achievement of objectives, such as operational units and support.
- **Establishes reporting lines.** Lines of reporting to effect authorities, responsibilities, and communication guide management activities. Organizing authority and accountability relationships among various functions provides reasonable assurance that work activities are aligned with agency objectives. Responsibilities can generally be viewed as being within three lines of defense against the failure to achieve agency objectives:
 - Management and other agency personnel provide the first line in their day-to-day activities, maintaining effective internal control over those activities.
 - Support functions typically ensure the proper functioning of internal controls through the services provided as the second line of defense.

Five Components of Internal Control

- Internal auditors, external auditors, and other independent parties provide the third line of defense by assessing and reporting on internal controls and recommending corrective actions or enhancements for management's consideration and implementation.
- **Defines, assigns, and limits authorities and responsibilities.** Management delegates authority, defines responsibilities, and uses appropriate processes and technology to segregate duties as necessary to various levels within the agency.

Principle Four:

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

Points of Focus

- **Establishes policies and practices.** Policies and practices reflect expectations of competence necessary to support the achievement of objectives.
- **Evaluates competence and addresses shortcomings.** Management evaluates competence across the agency and in outsourced service providers in relation to policies and practices, acting as necessary to address shortcomings.
- **Attracts, develops, and retains individuals.** The agency provides the mentoring and training needed to attract, develop, and retain sufficient and competent staff to support the achievement of objectives.
- **Plans and prepares for succession.** Management develops contingency plans for assignment of responsibility important for internal control.

Principle Five:

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

Points of Focus

- **Enforces accountability through structures, authorities, and responsibilities.** Management establishes mechanisms to communicate and hold individuals responsible for performance of internal control processes, implementing corrective action as necessary.
- **Establishes performance measures, incentives, and rewards.** Management determines performance measures to evaluate achievement, providing incentives and rewards to drive performance.

Five Components of Internal Control

- **Evaluates performance measures, incentives, and rewards for ongoing relevance.** Management aligns incentives and rewards with agency standards of conduct.
- **Considers excessive pressures.** Management evaluates and adjusts pressures associated with achievement of objectives as management assigns responsibilities, develops performance measures, and evaluates performance. Because goals and targets create pressure on staff, management may rebalance workloads or increase resources to reduce risk to the achievement of objectives.
- **Evaluates performance and rewards or disciplines individuals.** Standards of conduct and expected levels of performance are evaluated, considering rewards or disciplinary action as appropriate.

Risk Assessment

Risk is the possibility that an event will occur and adversely affect the achievement of objectives. Each agency faces a variety of risks from external and internal sources. Having established an effective control environment, management assesses risk and sets risk tolerance levels through established procedures. Each risk is evaluated in terms of its impact and likelihood of occurrence. Overall, risk assessment provides a basis for how risk will be managed.

Principles six through nine must be implemented and effectively working together to achieve the risk assessment internal control component.

Principle Six:
Management defines objectives clearly to enable the identification of risks and defines risk tolerances.

Points of Focus

Operations

- **Reflects management choices.** Objectives center around management's judgment, based on the nature of the services provided, stakeholder expectations, and other factors – each supported by specific criteria and measurement focus.
- **Considers tolerance for risk.** Management considers acceptable levels of variation in reaching objectives.
- **Includes operations and financial performance goals.** Within goals related to operations, management typically includes both desired levels of service delivery and corresponding financial measures.

Five Components of Internal Control

- **Forms a basis for committing resources.** Management uses operations objectives to define the level of resources needed to attain desired outcomes.

External Financial Reporting Objectives

- **Complies with applicable accounting standards.** The agency includes objectives that are applicable to its circumstances.
- **Considers materiality.** Management judges materiality based on qualitative and quantitative aspects, the needs of financial report users, and the size or nature of a misstatement.
- **Reflects agency activities.** External reporting reflects applicable agency transactions and events to show qualitative characteristics.

External Non-Financial Reporting Objectives

- **Complies with externally established standards and frameworks.** Management establishes objectives consistent with laws or regulations, industry practice, or other recognized measurement tools.
- **Considers the required level of precision.** Management considers the level of precision or accuracy suitable for user needs based on established criteria.
- **Reflects agency activities.** Management determines objectives based on the underlying transactions and events with a range of acceptable limits.

Internal Reporting Objectives

- **Reflects management's choices.** Internal reporting provides, at management's discretion, accurate and complete information needed to sufficiently operate the agency.
- **Considers the required level of precision.** Management considers the level of precision or accuracy suitable for agency needs.
- **Reflects agency activities.** Management determines objectives based on the underlying transactions and events with a range of acceptable limits.

Five Components of Internal Control

Compliance Objectives

- **Reflects external laws and regulations.** Laws, regulations, federal funding rules, and other authoritative guidance establish minimal standards of conduct the agency should integrate into compliance objectives.
- **Considers tolerance for risk.** Management considers the acceptable levels of variation relative to the achievement of compliance objectives.

Principle Seven:

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

Points of Focus

- **Includes agency-wide and subsidiary levels.** The agency identifies and assesses risk at the agency and major service or program levels.
- **Analyzes internal and external factors.** Internal factors considered may include the complex nature of the programs, organizational structure, or new technology uses. External factors may include new or amended laws or economic instability.
- **Involves appropriate levels of management.** Management puts into place effective mechanisms to identify, assess, and respond to risk, involving appropriate personnel throughout the agency.
- **Estimates significance of risks identified.** Analysis of impact and likelihood helps management prioritize identified risks.
- **Determines how to respond to risks.** The risk assessment considers how the risk should be managed and whether to accept, avoid, reduce, or share the risk.

Principle Eight:

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

Points of Focus

- **Considers types of fraud.** The assessment considers fraudulent reporting, possible loss of assets, and corruption resulting from the various ways fraud and misconduct can occur.
- **Assesses incentives and pressures.** Management considers employee motives to commit fraud.

Five Components of Internal Control

- **Assesses opportunities.** Assessment of fraud risk considers opportunities for unauthorized acquisition, use, or disposal of assets, altering of agency records, or committing other inappropriate acts.
- **Assesses attitudes and rationalizations.** The assessment considers how management and other personnel might engage in or justify inappropriate actions.

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

Points of Focus

- **Assesses changes in the external environment.** Risk identification considers changes in the regulatory, economic, and physical environment in which the agency operates.
- **Assesses changes in the business model.** The agency considers if new business lines impact the nature of services the agency provides, changes in stakeholder expectations, and/or technology advancements that impact future operations.
- **Assesses changes in leadership.** The agency considers if changes in management or respective attitudes and philosophies impact the system of internal control.

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. An integral part of the control activity component is segregation of duties.

Principles ten through twelve must be implemented and effectively working together to achieve the control activities internal control component.

Five Components of Internal Control

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

Points of Focus

- **Integrates with risk assessment.** Control activities align with risk assessment to ensure the risk response functions in an appropriate timely manner. Selecting control activities focuses on management decisions to reduce risk.
- **Considers agency-specific factors.** Management considers the business environment, complexity, scope of operations, and other characteristics which affect the selection and development of control activities.
- **Determines relevant business processes and transaction level controls.** Management considers all aspects of operations, including information technology (IT) and third-party service providers when determining the need for control activities.
- **Evaluates a mix of control activity types.** Management considers a range and variety of manual and automated controls, preventive, and detective controls. Examples of control activities include:
 - Authorizations and approvals to confirm validity of actions.
 - Verifications comparing two or more items with each other or against a policy for consistency.
 - Physical controls to safeguard assets or information such as locked storage areas.
 - Controls over standing data used to process transactions such as an approved vendor list.
 - Reconciliations comparing two or more items to identify differences.
 - Supervisory controls applicable in the circumstances.
- **Considers whether the proper level of control activities is applied.** To maximize the mitigation of risk, management ensures personnel at various levels perform control activities. Examples include analytical reviews to identify reasons when actual performance deviates from expected performance.

Five Components of Internal Control

- **Addresses segregation of duties.** Management divides or segregates duties among different people to reduce the risk of error or fraudulent actions. For instance, different persons perform responsibilities for asset custody, recording transactions related to assets, approving transactions or reconciling results. If segregation is not practical management develops compensating controls to mitigate risk to an acceptable level.

Principle Eleven:
Management designs the information system and related control activities to achieve objectives and respond to risks.

Points of Focus

- **Determines dependency between the use of technology in business processes and technology general controls.** Management understands and determines the dependency and linkage between business processes, automated control activities, and technology general controls.
- **Establishes relevant technology infrastructure control activities.** Management selects and develops control activities over the technology infrastructure, which are designed and implemented to help ensure the completeness, accuracy, and availability of technology processing.
- **Establishes relevant security management process control activities.** Management selects and develops control activities designed and implemented to restrict technology access rights to authorized users commensurate with job responsibilities and to protect the assets from external threats.
- **Establishes relevant technology acquisition, development, and maintenance process control activities.** Management selects and develops control activities over the acquisition, development, and maintenance of technology and its infrastructure to achieve objectives.

Principle Twelve:
Management implements control activities through policies.

Points of Focus

- **Establishes policies and procedures to support deployment of management directives.** Management establishes control activities built into business processes and day-to-day operations through policies and standard operating procedures to accomplish objectives.

Five Components of Internal Control

- **Establishes responsibility and accountability for executing policies and procedures.** Management addresses responsibility to carry out policies and standard operating procedures, holding individuals accountable for carrying out management's directives.
- **Performs in a timely manner.** Standard operating procedures identify the timing of the control activity and necessary follow-up actions. Untimely procedures reduce control activity effectiveness.
- **Takes corrective action.** Responsible personnel investigate and act upon anomalies identified during control activity processes.
- **Performs using competent personnel.** An effective internal control activity depends on competent personnel with sufficient authority to perform the activity.
- **Reassesses policies and procedures.** The agency periodically evaluates the relevance and effectiveness of policies and standard operating procedures. Changes in personnel, processes, technology, and other variables may reduce effectiveness or make other control activities redundant.

Considerations for Designing and Implementing Control Activities

When designing and implementing control activities, management appraises the cost versus benefit of the activity with a goal to achieve the maximum benefit at the lowest possible cost. The cost of the control activity should not exceed the benefit derived from the control or the impact on the agency if the undesirable event occurred. To ensure maximum effectiveness, the agency will prioritize risks based on the impact and likelihood of the risks, and focus resources on the design and implementation of control activities based on the prioritization.

Information and Communication

Quality information from both internal and external sources supports the functioning of the other components of internal control. Continual communication processes provide, share, and obtain necessary information to achieve objectives. Internal communication sends a clear message to personnel about goals, objectives, standard operating procedures, and the importance of internal control responsibilities. External communication effectively conveys information to outside parties and internalizes information received from outside sources.

Five Components of Internal Control

Principles thirteen through fifteen must be implemented and effectively working together to achieve the information and communication internal control component.

Principle Thirteen:
Management uses quality information to achieve objectives.

Points of Focus

- **Identifies information requirements.** A process exists to identify the information required to support the functioning of internal control and achievement of objectives.
- **Captures internal and external sources of data.** Management considers a comprehensive scope of potential events or activities and determines the most relevant useful information and data sources.
- **Processes relevant data into information.** The agency develops information systems to source, capture, and process data into meaningful actionable information. Information systems include a combination of people, processes, data, and technology.
- **Maintains quality throughout processing.** Quality information may be described as accessible, available, complete, accurate, correct, current, protected, retained, sufficient, timely, valid, and verifiable.
- **Considers cost and benefits.** The nature, quantity, and precision of information communicated are commensurate with and support the achievement of objectives.

Principle Fourteen:
Management internally communicates the necessary quality information to achieve agency objectives.

Points of Focus

- **Communicates internal control information.** A process exists to communicate required information to enable all agency personnel to understand and carry out internal control responsibilities. The type of information may take the form of policies and procedures, specified objectives, job duties and responsibilities, performance management competencies and performance factors, and many others.
- **Communicates with leadership.** Agency management communicates with leadership to ensure all parties have the information needed to fulfill roles and responsibilities.

Five Components of Internal Control

- **Provides separate communication lines.** Communication channels, such as whistle-blower hotlines or similar mechanisms, exist to enable anonymous or confidential communications when the normal channels are inoperative or ineffective.
- **Selects relevant method of communication.** Management uses a variety of processes to ensure the clarity and effectiveness of communications. Communication can take the form of letters, emails, dashboards, presentations, social media postings, webcasts, face-to-face meetings, policies and procedures, performance evaluations, and others.

*Principle Fifteen:
Management externally communicates the necessary quality information to achieve agency objectives.*

Points of Focus

- **Communicates to external parties.** Processes are in place to communicate relevant and timely information to external parties, including customers, regulators, federal cognizant agencies, and other stakeholders.
- **Enables inbound communications.** Open communication channels exist to solicit input from external stakeholders. Inbound communication aids with obtaining feedback on services, notice of new laws or regulations, results from audits, vendor questions, and a variety of other types of inbound information which assists the agency with assessing the functioning of internal control.
- **Communicates with Leadership.** Relevant information is provided to assist with fulfilling oversight responsibilities.
- **Provides separate communication lines.** Like internal channels, external channels exist to enable anonymous or confidential communications when the normal channels are inoperative or ineffective, for example whistle-blower hotlines or similar mechanisms.
- **Selects relevant method of communication.** The method by which management communicates externally affects the ability to obtain needed information as well as ensuring key messages are received and understood. Management considers and selects the appropriate method of communication, given the audience, nature of the message, timing, and other factors.

Five Components of Internal Control

Monitoring

The monitoring component evaluates whether each of the five components of internal control is present and functioning. As a dynamic process, internal control must be continually adapted to the risks and changes the agency faces. Monitoring aligns the internal control system with changing objectives, environment, laws, resources, and risks. Internal control monitoring assesses the quality of performance over time and promptly resolves the findings of audits and other reviews. Improvements and corrective actions complement control activities in achieving objectives.

Principles sixteen and seventeen must be implemented and effectively working together to achieve the monitoring internal control component.

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

Points of Focus

- **Considers a mix of ongoing and separate evaluations.** Ongoing evaluations performed through day-to-day operations in real time provide timely feedback for quick response. Separate evaluations conducted periodically vary in scope and frequency depending on risk assessment and the results of ongoing evaluations.
- **Considers rate of change.** The frequency of change in business processes or environment impact whether ongoing or periodic evaluations are most appropriate.
- **Establishes baseline of understanding.** The agency creates a baseline of information for use when developing ongoing and separate evaluations. Deviations from the baseline, noted during monitoring, may indicate areas of concern that need further assessment.
- **Uses knowledgeable personnel.** Persons involved with monitoring activities possess knowledge needed to understand the monitoring process.
- **Integrates into business processes.** Ongoing evaluations are built into business processes and adjusted to changing conditions, often using technology.

Five Components of Internal Control

- **Adjusts scope and frequency.** The agency varies the scope and frequency of evaluations depending on risk.
- **Objectively evaluates.** Evaluations involve objective feedback to maximize effectiveness.

Principle Seventeen:
Management remediates identified internal control deficiencies on a timely basis.

Points of Focus

- **Assesses results.** By assessing monitoring results, management may receive assurance that the internal control system is functioning properly or identify potential improvements for the internal control system.
- **Communicates deficiencies.** Management communicates potential improvements or deficiencies to appropriate personnel for remediation on a timely basis.
- **Monitors corrective actions.** Management tracks progress on the progress of improvements or resolution of deficiencies. Persons responsible for tracking corrective action should differ from those conducting the monitoring activities.

Uniform Compliance Guidelines on Internal Controls for State and Quasi Agencies

<p>Part Two: Evaluation and Development of the Agency Internal Control System</p> <p>Section One: Control Environment</p>	<p>Issue Date: April 11, 2024</p>
	<p>Revision Date:</p>

Table of Contents

Overview	33
Why It Matters	33
Where to Start	34-35
Developing the Control Environment	35-39
Set the Tone at the Top.....	36
Define and Communicate Standards of Conduct	36-37
Evaluate Adherence to Standards of Conduct.....	37
Establish Oversight Structure and Procedures for the Internal Control System.....	37
Design Agency Organizational Structure	38
Recruit, Develop, and Retain Competent Staff.....	38
Create Succession and Contingency Plans.....	39
Promote Accountability.....	39
Documenting the Agency Control Environment	39-40

Section One: Control Environment

Overview

The control environment forms the foundation for a strong internal control system. Management sets the tone for a solid foundation by prioritizing internal controls and communicating the importance of internal controls throughout the agency.

Five principles are associated with the control environment:

Principle One: The agency demonstrates a commitment to integrity and ethical values.

Principle Two: Agency leadership oversees the internal control system.

Principle Three: Management establishes an organizational structure, assigns responsibility, and delegates authority to achieve agency objectives.

Principle Four: The agency demonstrates a commitment to attract, develop, and retain competent individuals.

Principle Five: Management evaluates performance and holds individuals accountable for their internal control responsibilities.

A strong control environment calls for ongoing commitment, communication, and vigilance throughout the agency. Because it includes the overall attitude and actions of management regarding internal controls, the control environment does not generally change with a given objective.

Why It Matters

The control environment promotes a culture of integrity, ethics, and accountability which contributes to the long-term success of the agency's achievement of objectives. For instance, when management communicates a clear message about the importance of internal controls, ethics, and accountability, it –

- encourages employees to adopt agency values and expectations.
- provides employees with a framework to make decisions that align with agency values.
- reduces the likelihood of fraud, errors, and compliance issues by defining proper procedures.
- promotes accountability by documenting processes, responsibilities, and actions.
- provides a method for addressing and resolving issues.

Section One: Control Environment

Where to Start

Evaluating the agency control environment serves as the optimal starting point for developing a successful internal control system. After evaluation, additional controls may be developed by following suggested steps under "Developing the Control Environment" or other processes determined by management. To be effective, the internal control system must be documented.

Evaluating the Agency Control Environment

Does the agency have documented control environment policies and procedures? Internal Control evaluation involves conducting periodic assessments of the agency's internal controls to determine whether –

- The agency will likely achieve its objectives.
- Risks to the agency and opportunities for improvement are identified.
- The elements of the agency's internal control system are functioning effectively.

Evaluation presents an opportunity to discuss and document the control environment – and establish the tone at the top. Meaningful and successful evaluations combine input from leadership across the agency, including major department or program areas. During this process, the consideration of absent controls will strengthen the control environment and facilitate an action plan for the design and implementation of a full-bodied control environment.

Tools for Evaluation. Part Three contains optional tools for management to use in the evaluation of agency internal controls. Management may **choose one** of the available tools or consider other methods of evaluation based on the needs of the agency.

Control Environment Self Evaluation Questionnaire. A series of self-evaluation questions will guide management through major internal control considerations in a "yes or no" format, which will help management determine which areas need further development. [\[Link\]](#)

Section One: Control Environment

Control Environment Internal Control Evaluation Template. This spreadsheet identifies common best practices for the control environment. A series of open-ended self-evaluation questions will guide management through major internal control considerations with the ability to designate current controls as sufficient, needing improvement, or nonexistent. [\[Link\]](#)

Based on the evaluation of the control environment, management may consider developing the control environment by following the recommended steps in "Developing the Control Environment."

Developing the Control Environment

A positive and supportive attitude toward internal control and conscientious management sets the tone for the control environment.

Through the evaluation process, management may decide that internal controls sufficiently address all principles or need further development.

A full-bodied internal control system addresses each internal control principle. The following steps, organized by principle, may be considered by management in the development of the control environment.

1. Set the Tone at the Top
2. Define and Communicate Standards of Conduct
3. Evaluate Adherence to Standards of Conduct
4. Establish Oversight Structure and Procedures for the Internal Control System
5. Design Agency Organizational Structure
6. Recruit, Develop, and Retain Competent Staff
7. Create Succession and Contingency Plans
8. Promote Accountability

Tools for Development. Part Three contains optional tools for management to use in developing the agency control environment. Management may **choose one** of the available tools or other method suitable for the agency's needs.

Control Environment Development Questionnaire. This document walks through the steps in "Developing the Control Environment" with examples of activities to improve the control environment and space to document controls or references to agency policies.

Section One: Control Environment

Control Environment Development Template. This template provides an abbreviated method for management to design control environment processes by following the steps in "Developing the Control Environment" and document controls or references to agency policies.

Principle One:

The agency demonstrates a commitment to integrity and ethical values

- 1. Set the Tone at the Top.** Management's directives, attitudes, and behaviors reflect the integrity and ethical values expected throughout the agency and the state. The Agency Head and management set an appropriate tone at the top by demonstrating the importance of integrity and ethical values; leading by example; and reinforcing the commitment to do quality work.

Specific ways to set the tone at the top include –

- Discussing expected behaviors regularly at staff meetings.
- Formalizing expectations in agency and statewide documents, such as the agency mission statement, core values, and strategic plan.
- Placing importance on the State Ethics Code.
- Reinforcing expectations of compliance with State Personnel Policies.

- 2. Define and Communicate Standards of Conduct.** Part of the commitment to integrity and ethical values includes defining standards of conduct to inform employees about expected behaviors. Enterprise-wide policies and standards of conduct include –

- Indiana State Employee Handbook
- Indiana State Personnel Department Standardized Policies
- State Ethics Code
- Information Technology Resources Policy

Each agency also should consider its own policies and procedures to address expectations regarding business practices and ethical behavior, such as –

- Remote Work
- Continuing Professional Education requirements
- Dress Code

Section One: Control Environment

Once defined, standards of conduct must be communicated to employees, for example, through agency newsletter, regular staff meetings, training videos, one-on-one meetings, etc.

3. Evaluate Adherence to Standards of Conduct. Gauging adherence to standards of conduct addresses differences between actual performance and expected standards. For example –

- Regular evaluations with meaningful feedback.
- Clear consistent disciplinary policies and procedures.
- Established methods of reporting noncompliance, misconduct, or fraud without retribution.
 - Agency channels for employees to report noncompliance, misconduct, or fraud.
 - Indiana Office of Inspector General Hotline.
 - State Board of Accounts Fraud Reporting Form.

*Principle Two:
Agency leadership
oversees the internal
control system.*

4. Establish Oversight Structure and Procedures for the Internal Control System. For most agencies, the agency head, or a statutory board provides oversight of the internal control system. Oversight enables the agency to fulfill responsibilities in laws and regulations, government guidance, and feedback from key stakeholders. Specifically, leadership oversees the agency's operations and makes oversight decisions so that the agency achieves its objectives in alignment with integrity and ethical values.

Leadership oversees the design, implementation, operation, and monitoring of the internal control system, and provides input to resolve deficiencies. Procedures might be –

- Having periodic meetings and other communications with management.
- Maintaining appropriate documentation of meetings, including agendas and minutes.
- Reviewing management's internal control documentation.
- Reviewing management's corrective action plans.
- Following up to ensure deficiencies have been corrected, including audit findings.
- Completing the Internal Control Certification required by FMC 6.1.
- Ensuring performance of the Annual Risk Assessment per FMC 6.2.
- Ensuring response to OMB entity-wide risk self-assessment questionnaires.

Section One: Control Environment

Principle Three:

Management establishes an organizational structure, assigns responsibility, and delegates authority to achieve agency objectives.

5. Design Agency Organizational Structure. Designing the organizational structure and assigning responsibility enables the agency to plan, execute, control, and assess the achievement of objectives. Examples include steps to –

- Establish, document, review, and update an organizational plan that clearly addresses the assignment of authority and responsibility, such as an organizational chart.
- Ensure that job descriptions clearly detail responsibilities.
- Delegate authority, assign responsibility, and design controls with proper segregation of duties or compensating controls.
- Develop standard operating procedures to communicate responsibilities to personnel and provide a method to monitor and evaluate controls.

Principle Four:

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

6. Recruit, Develop, and Retain Competent Staff. Policies pertaining to recruitment, training, mentoring, and retention of personnel consider agency objectives and emphasize competency. Competency requires relevant knowledge, skills, and abilities gained from professional experience, training, and certifications to carry out assigned responsibilities and understand the importance of internal control. Incorporated practices –

- Reinforce basic minimum requirements in job descriptions, such as educational prerequisites.
- Document expectations in personnel performance management documents.
- Evaluate employee performance of job responsibilities.
- Develop competencies appropriate for key roles.
- Mentor by guiding performance, aligning skills with agency objectives, and helping personnel adapt to an evolving environment.
- Motivate by reinforcing expected levels of performance and desired conduct, including training and credentialing. For example, State policies on training opportunities through SuccessFactors, LinkedIn Learning, Tuition Support, etc.

Section One: Control Environment

- 7. Create Succession and Contingency Plans.** Over the long term, management defines plans relating to the replacement of personnel in key roles to enable the agency to achieve objectives through times of turnover and emergency. To do this, management may consider,
- Training succession candidates through job shadowing and cross training.
 - Encouraging knowledge sharing.
 - Maintaining written plan documents, including standard operating procedures.

Principle Five:

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

- 8. Promote Accountability.** Tone at the top drives accountability. Individuals are held accountable for their internal control responsibilities through a recognized, understood structure which incorporates corrective action procedures. Methods include –
- Regular meetings to verify performance of internal control responsibilities.
 - Formal performance appraisals and improvement plans.
 - Assessment and rebalancing of excessive pressures and workload through regular meetings with staff.
 - Maintaining appropriate documentation of meetings, including agendas and minutes.

Documenting the Agency Control Environment

The agency control environment must be documented. Documenting the agency's internal control system fosters communication and understanding of the internal control system. Benefits encompass the capability to –

- Communicate the design, implementation, and operating effectiveness of the internal control system to personnel.
- Retain organizational knowledge and mitigate the risk of having knowledge limited to a few personnel.
- Support the results of ongoing monitoring, identify internal control issues, and support the appropriate corrective actions.

Section One: Control Environment

- Provide tangible audit evidence to internal and external assurance providers. As part of the audit engagement, auditors will ask for written internal controls, and test those controls to determine the nature, timing, and extent of audit testing. Written internal controls must incorporate a process to maintain tangible evidence that the controls are functioning as intended. For example, auditors may review the organizational chart and standard operating procedures for assignment of responsibility.

Methods to document the internal control system include narratives, flowcharts, and standard operating procedures. Part Three contains optional tools to facilitate and document the evaluation and development of internal controls.

Uniform Compliance Guidelines on Internal Controls for State and Quasi Agencies

<p>Part Two: Evaluation and Development of the Agency Internal Control System</p> <p>Section Two: Risk Assessment</p>	<p>Issue Date: April 11, 2024</p>
	<p>Revision Date:</p>

Table of Contents

Overview	43
Why It Matters	43
Where to Start	44
Conducting a Risk Assessment	45-52
Define the Agency’s Mission Statement and Related Objectives	45-47
Identify Risks to the Achievement of Objectives	47-48
Prioritize Identified Risks	48-49
Respond to the Identified Risks	49-50
Consider the Potential for Fraud	50-51
Identify and Assess Risk from Change	52
Documenting the Risk Assessment Process	53

Section Two: Risk Assessment

Overview

What could go wrong? This question forms the basis for risk assessment. Risk is the possibility that an event will occur and adversely affect the achievement of objectives. Management employs a risk assessment process to identify, analyze, and manage the potential risks that could hinder or prevent the achievement of objectives.

Risks vary in significance. A successful risk assessment prioritizes key activities and controls by combining input from leadership across the agency, including major department or program areas.

Principles six through nine correspond to the risk assessment component.

Principle Six: Management defines objectives clearly to enable the identification of risks and defines risk tolerances.

Principle Seven: Management identifies, analyzes, and responds to risks related to achieving the defined objectives.

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

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

Why It Matters

Over the course of a day, a week, a month, or a year, situations occur which could hinder or prevent an agency from fulfilling responsibilities and meeting objectives. Because of this possibility, successful managers continually identify and analyze potential risks. Performing risk assessments assist managers in prioritizing the activities where controls are needed most. Management uses risk assessments to determine the potential for loss in programs and functions and to design the most cost-effective and productive internal controls. Risk assessment improves the agency in many ways by identifying events that may hinder operational, reporting, and compliance objectives. This results in –

- Improved decision making through sound planning and the systematic setting of objectives.
- Strengthened internal control for high-risk activities.
- Improvement in services and mitigation of potential disruptions.
- Alignment of processes with agency mission and objectives, increasing efficiency and effectiveness.

Section Two: Risk Assessment

Where to Start

The first step in conducting a risk assessment involves reviewing the agency's mission and related objectives. Based on agency objectives, the risk assessment process identifies and prioritizes risks to agency objectives and decides on the proper response to the identified risks. "Conducting a Risk Assessment" in this section provides suggested steps.

Evaluating the Risk Assessment Process

After the risk assessment is completed, the management should evaluate the processes used. Internal control evaluation involves conducting periodic assessments of the agency's internal controls to determine whether –

- The agency will likely achieve its objectives.
- Risks to the agency and opportunities for improvement are identified.
- The elements of the agency's internal control system are functioning effectively.

Evaluation presents an opportunity to discuss and document the processes used to conduct the risk assessment. Meaningful and successful evaluations combine input from leadership across the agency, including major department or program areas. Evaluating the actual risk assessment process helps management make improvements which will best serve the needs of the agency. During this process, the consideration of absent controls will strengthen the component and facilitate an action plan for the design and implementation of a full-bodied risk assessment component.

Tool for Evaluation. Part Three contains an optional tool for management to use in the evaluation of the agency risk assessment process. Management may consider other methods of evaluation based on the needs of the agency.

Risk Assessment Internal Control Evaluation Template. This spreadsheet identifies common best practices for the risk assessment component. A series of open-ended self-evaluation questions will guide management through major risk assessment process considerations with the ability to designate current processes as sufficient, needing improvement, or nonexistent. [\[Link\]](#)

Management may follow the evaluation with implementation and documentation of improvements, if needed.

Section Two: Risk Assessment

Conducting a Risk Assessment

Risk assessment involves an ongoing process to recognize potential problems (risks) and determine the best way to manage them.

A full-bodied internal control system addresses each internal control principle. The following steps, organized by principle, may be considered by management for conducting a risk assessment.

1. Define the Agency's Mission Statement and Related Objectives
2. Identify Risks to the Achievement of Objectives
3. Prioritize Identified Risks
4. Respond to the Identified Risks
5. Consider the Potential for Fraud
6. Identify and Assess Risk from Change

Tools for Conducting a Risk Assessment.

Part Three contains an optional tool for management to use in conducting a risk assessment. Management may choose other methods based on the needs of the agency.

Risk Assessment Template. The Risk Assessment Template provides a method for management to document risks to objectives and management's response to those risks. This template follows the outlined steps in "Conducting a Risk Assessment."

Example Objectives, Risks, Controls. This document provides examples of objectives, risks, and key controls for major transaction areas. Lists are not intended to be exhaustive or applicable to all agencies. [\[Link\]](#)

Each major transaction area may include some or all the following examples –

- Example Objectives and Risks.
- Minimum Internal Control Standards per the Accounting and Uniform Compliance Guidelines Manual for State and Quasi Agencies.
- Example Key Controls.

Principle Six:
Management defines objectives clearly to enable the identification of risks and defines risk tolerances.

1. Define the Agency's Mission Statement and Related Objectives

Internal control focuses on the achievement of the agency mission and the underlying objectives associated with major service areas or transaction levels.

Section Two: Risk Assessment

Agency Mission

To identify risks to agency-wide objectives, start with defining the agency mission statement. A mission statement broadly articulates the fundamental purpose and long-term vision, serving as the foundation for agency goals and objectives.

Major Service Area or Transaction-level Objectives

Objectives flow from the agency mission statement based on external requirements, such as laws, regulations and standards, and internal policies and expectations from the control environment. An objective is a specific, measurable, time-bound goal that answers the question: *What specific, measurable outcome or result do we want to achieve?*

By setting objectives at the major service areas and transaction levels, an agency can identify critical success factors - key things that must go right for the agency to meet objectives. During the risk assessment process, the agency determines critical activities to manage risks and ensure achievement of the agency mission and core business objectives.

Objectives fall into one of the three categories: Operations, Compliance, and Reporting.

Operations Objectives pertain to the effectiveness and efficiency of operations. Operations objectives will reflect the agency's mission, incorporating operations and financial performance goals.

As a starting point, management may identify key agency-wide objectives and critical major service areas or transaction level objectives. A brainstorming session with leadership and management together should bring key critical objectives to the forefront. Work through the risk assessment process for the most critical operations objective(s). Then work toward other significant operations objectives identified during the risk assessment process.

Compliance Objectives relate to compliance with applicable laws and regulations. Compliance objectives encompass requirements contained in federal laws, including Uniform Guidance (Title 2 CFR 200), Indiana Code, State Budget Agency Financial Management Circulars, State Board of Accounts Uniform Compliance Guidelines, or other authoritative sources.

Section Two: Risk Assessment

For compliance objectives, management may wish to begin by assessing risks to compliance with major federal program requirements, unresolved audit findings, and management letter comments. Then, work toward other significant compliance requirements identified during the risk assessment process.

Reporting Objectives pertain to the reliability of reporting for internal or external purposes, such as financial statements, financial schedules, program reports, etc.

As a beginning point, identify an inventory of required financial reports. Start by focusing on the most significant reporting requirements, such as financial information for the ACFR (Annual Comprehensive Financial Report) and federal grants. Then work toward other significant reporting requirements identified during the risk assessment process.

Principle Seven:

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

2. Identify Risks to the Achievement of Objectives

After defining objectives, the next step will identify risks that would threaten the accomplishment of each objective. This analysis considers the question, "What can go wrong?" And, it may also consider the question, "What opportunities are we missing?"

Risks can be internal, such as human error, fraud, and changes in technology; or external, like changes in legislation or program requirements, and public emergencies. Whether internal or external, risk assessment considers inherent risk, fraud risk, and change risk.

- **Inherent Risk.** Inherent risk is the level of risk that exists in a process or activity before actions to alter the risk's impact or likelihood. Activities with inherent risk have a greater potential for errors, loss, waste, unauthorized use, or misappropriation due to the nature of the activity or asset.

Examples of inherently risky activities include cash receipts, complex programs or activities, services provided through sub-recipients or vendors, direct third-party beneficiaries, and unresolved audit findings.

Section Two: Risk Assessment

- **Fraud Risk.** Fraud risk considers risk of deceptive activities to obtain money, property, or services; to avoid payment or loss of services; or to secure personal or business advantage. Waste and abuse would also be recognized as part of this category. Principle eight specifically addresses Fraud Risk.
- **Change Risk.** When change occurs, it often affects the control activities that were designed to prevent or reduce risk. Principle nine covers Change Risk.

3. Prioritize Identified Risks

To effectively allocate limited resources, management must gain a comprehensive understanding of the identified risks by prioritizing the risks in terms of likelihood and impact.

Likelihood

For each identified risk, management rates the likelihood of the event in terms of low, medium, or high.

- **Low.** The risk event is unlikely to occur.
- **Medium.** The risk event is more likely to occur than unlikely.
- **High.** The risk event is highly likely or reasonably expected to occur (or ongoing).

Impact

For each identified risk, management assesses the risk in terms of potential impact if the risk event were to occur. Impact addresses the question, "*What are the consequences?*"

Impact spans the categories of insignificant, minor, serious, disastrous, or catastrophic.

- **Insignificant.** The impact will not significantly affect the ability to achieve objectives. For example, the risk of immaterial noncompliance or immaterial errors.
- **Minor.** For example, immaterial misstatements to the financial statements.
- **Serious.** The impact could significantly affect the agency's ability to achieve objectives. For example, audit findings of noncompliance or lack of documentation to support financial reporting.

Section Two: Risk Assessment

- **Disastrous.** For example, audit questioned costs, material misstatements to the financial statements.
- **Catastrophic.** The impact could preclude or highly impair the agency's ability to achieve objectives. For example, material loss of federal fundings or failure to maintain financial records.

Rating

The combination of the two factors of likelihood and impact provides management with a rating for each risk identified. Rank risks in a logical manner, from most significant (high impact) and most likely to occur (high likelihood) to the least significant (low impact) and least likely (low likelihood).

Documentation

Examples of documentation for likelihood and impact ratings would include relevant criteria such as financial projections, historical examples, expert opinions, statistical analysis. A narrative description might be used to summarize key points for each risk.

Management may decide to incorporate a risk matrix, heat map, or similar visual tool to assess and classify risks based on likelihood and impact.

4. Respond to the Identified Risks

After prioritizing risks, management next determines how to respond and manage those risks. For example, management may accept, avoid, reduce, or share the risk. Residual risk equals the remaining risk after management's response to the risk.

- **Accept** – Management acknowledges the risk but makes a deliberate decision to retain the risk, usually due to risk insignificance or costly mitigation.
- **Avoid** – Management eliminates the risk. For example, requiring customers to pay fees online to avoid the risks inherent to accepting cash or checks.

Section Two: Risk Assessment

- Reduce – Management takes action to bring the risk down to a manageable level by designing internal controls to prevent or detect the risk event - for example segregation of duties, review, or authorization procedures.
- Share – Management shares the risk by transferring the risk to another party, for example the purchase of insurance.

In many cases, management may already have controls in place to reduce the risk to an acceptable level. Key controls should be documented and evaluated on a regular basis for adequacy.

Retaining analysis and interpretation of the risk assessment information will facilitate periodic review of decisions to determine whether changes in conditions warrant a different approach to managing risk.

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

5. Consider the Potential for Fraud

As part of the risk assessment process, fraud must be considered - such as fraudulent financial reporting, misappropriation of assets, and illegal acts. In addition to fraud, assess the likelihood of other types of misconduct such as waste or abuse.

Once identified, management must prioritize and respond to fraud risks.

Fraud

The Green Book defines fraud as "obtaining something of value through willful misrepresentation." Intent distinguishes fraud from a weakness in internal control. Fraud risk assessment specifically identifies possibilities for intentional acts to misstate financial information, misappropriate assets, or engage in corruption.

- Fraudulent Financial Reporting occurs through intentional misstatements or omissions of amounts or disclosures in financial statements to deceive financial statement users. For example, intentional alteration of accounting records, misrepresentation of transactions, or intentional misapplication of accounting principles.
- Misappropriation of Assets includes theft of assets, embezzlement of receipts, or fraudulent payments.
- Corruption encompasses bribery and other illegal acts

Section Two: Risk Assessment

Fraud can be internal or external. Internal fraud occurs when an employee, manager, or executive commits fraud against the agency. External fraud occurs when an outside party commits fraud against the agency. Fraud risks such as bribery and fraudulent reporting should be considered in relation to regulators, vendors, health care providers, regulated entities, grantees, subrecipients, and any other third parties.

Understanding why individuals commit fraud helps in assessing risk and establishing controls. Individuals generally commit fraud due to pressure, opportunity, and rationalization, commonly referred to as the fraud triangle.

- Pressure describes financial or emotional force pushing towards fraud. For example, a family member loses their job, their house forecloses, or medical bills pile up.
- Opportunity denotes the ability to execute fraud without being caught. Effective internal controls reduce opportunity.
- Rationalization comes through personal justification of dishonest actions. When seeing themselves as victims of unusual circumstances, individuals will develop an explanation making the illegal behavior acceptable.

Waste and Abuse

In addition to fraud risk, other forms of misconduct can occur, such as waste and abuse. Waste and abuse do not necessarily involve fraud or illegal acts.

Waste covers the act of using or expending resources carelessly, extravagantly, or for no purpose.

Abuse involves deficient or improper behavior when compared with the behavior a prudent person would consider reasonable and necessary in the circumstances. Abuse also includes the misuse of authority or position for personal gain or for the benefit of another.

Section Two: Risk Assessment

Principle Nine:

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

6. Identify and Assess Risk from Change.

The risk to reaching objectives increases dramatically during a time of change. New threats, opportunities, technology, regulatory requirements, funding challenges, and personnel changes all effect stress on the internal control system. Identify and adjust for significant changes which could alter agency objectives.

As part of the risk assessment process, ask the question, "*What has changed this year?*"

Once identified, management must prioritize and respond to change risks. Examples of external and internal circumstances that expose an agency increased risk include –

- Changing economic and political conditions
- Changes in State or Federal Regulation or Requirement
- New technology
- New accounting standards
- Changes in personnel
- New or modified technology
- New programs or services
- Reorganization
- Rapid growth
- Increased delegation of spending authority
- Moving to a new location

Section Two: Risk Assessment

Documenting the Risk Assessment Process

The Risk Assessment Process must be documented. Documenting the agency's internal control system fosters communication and understanding of the internal control system. Benefits encompass the capability to –

- Communicate the design, implementation, and operating effectiveness of the internal control system to personnel.
- Retain organizational knowledge and mitigate the risk of having knowledge limited to a few personnel.
- Support the results of ongoing monitoring, identify internal control issues, and support the appropriate corrective actions.
- Provide tangible audit evidence to internal and external assurance providers. As part of the audit engagement, auditors will ask for written internal controls, and test those controls to determine the nature, timing, and extent of audit testing. Written internal controls must incorporate a process to maintain tangible evidence that the controls are functioning as intended. For example, auditors may review the agency risk assessment for documented decisions related to prioritization and response to identified risks to the achievement of objectives.

Methods to document the internal control system include narratives, flowcharts, and standard operating procedures. Part Three contains optional tools to facilitate and document the evaluation and development of internal controls.

Uniform Compliance Guidelines on Internal Controls for State and Quasi Agencies

<p>Part Two: Evaluation and Development of the Agency Internal Control System</p> <p>Section Three: Control Activities</p>	<p>Issue Date: April 11, 2024</p>
	<p>Revision Date:</p>

Table of Contents

Overview	57
Why It Matters	57
Where to Start	57-58
Developing Agency Control Activities	58-68
Respond to Risks.....	60
Design Control Activities	61-65
Specifically Address the Information System	65-67
Document Control Activities	67
Communicate Responsibility	67
Review Policies and Procedures	68
Documenting Control Activities	68

Section Three: Control Activities

Overview

Control activities detect, prevent, or reduce identified risks that interfere with the achievement of objectives. Control activities include segregation of duties, review and approval processes, reconciliations, verifications, and asset security.

The Control Activities component consists of three principles.

Principle Ten: Management designs control activities to achieve objectives and respond to risks.

Principle Eleven: Management designs the information system and related control activities to achieve objectives and respond to risks.

Principle Twelve: Management implements control activities through policies.

Why It Matters

Control activities drive the agency's overall success, helping to manage risk, ensure compliance, and encourage efficiency and accountability. Effective control activities –

- Promote orderly, economical, efficient, and effective operations.
- Produce quality products and services consistent with the agency mission.
- Safeguard resources against loss due to waste, abuse, mismanagement, errors, and fraud.
- Promote adherence to statutes, regulations, uniform compliance guidelines, and procedures.
- Develop and maintain reliable financial and management data, and accurately report that data in a timely manner.
- Reduce the risk of mistakes and inappropriate actions through segregation of duties.
- Help personnel perform assigned responsibilities through documented policies and procedures.

Where to Start

Evaluating the agency control activities serves as the optimal starting point for developing a successful internal control system. After evaluation, additional controls may be developed by following suggested steps in "Developing Agency Control Activities" or other processes determined by management. To be effective, the internal control system must be documented.

Section Three: Control Activities

Evaluating the Agency Control Environment

Does the agency have documented control activity policies and procedures? Internal control evaluation involves conducting periodic assessments of the agency's internal controls to determine whether -

- The agency will likely achieve its objectives.
- Risks to the agency and opportunities for improvement are identified.
- The elements of the agency's internal control system are functioning effectively.

Evaluation presents an opportunity to discuss and document internal controls. Meaningful and successful evaluations combine input from leadership across the agency, including major department or program areas. During this process, the consideration of absent controls will strengthen control activities and facilitate an action plan for the design and implementation of a full-bodied internal control system.

Tools for Evaluation. Part Three contains an optional tool for management to use in the evaluation of agency control activities. Management may choose this tool or consider other methods of evaluation based on the needs of the agency.

Control Activities Internal Control Evaluation Template. This spreadsheet identifies common best practices for the control activities component. A series of open-ended self-evaluation questions will guide management through major internal control considerations with the ability to designate current controls as sufficient, needing improvement, or nonexistent. [\[Link\]](#)

Based on the evaluation of control activities, management may consider developing additional control activities by following the recommended steps in "Developing Agency Control Activities."

Developing Agency Control Activities

After identifying and assessing risks, management develops methods to minimize key risks. Control activities are actions and tools established through policies and procedures that prevent or detect identified risks to the achievement of objectives.

Through the evaluation process, management may decide that internal controls need improvement.

Section Three: Control Activities

A full-bodied internal control system addresses each internal control principle. The following steps, organized by principle, may be considered by management in the development of control activities.

1. Respond to Risks
2. Design Control Activities
3. Specifically Address the Information System
4. Document Control Activities
5. Communicate Responsibility
6. Review Policies and Procedures

Tools for Development. Part Three contains optional tools for management to use in developing agency control activities. Management may **choose one** tool or other method suitable for the agency's needs.

Control Development Questionnaire. This document walks through the steps outlined in "Developing Agency Control Activities" with examples of control activities and space to document controls or reference standard operating procedures.

Control Development Template. This spreadsheet provides an abbreviated method for management to design control activities which address specific risks identified through the risk assessment process. This template follows steps outlined in "Developing Agency Control Activities."

Example Objectives, Risks, Controls. This document provides examples of objectives, risks, and controls for major transaction areas. Lists are not intended to be exhaustive or applicable to all agencies. [\[Link\]](#)

Each major transaction area may include some or all the following examples –

- Example Objectives and Risks.
- Minimum Internal Control Standards per the Accounting and Uniform Compliance Guidelines Manual for State and Quasi Agencies.
- Example Key Controls.

Section Three: Control Activities

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

- 1. Respond to Risks.** Once risks are identified and assessed through the risk assessment process, management minimizes risks through control activities. When deciding the best response, management must use risk assessment information to identify the most effective and efficient control activities available for handling the risk. In addition to agency-specific factors, management should consider the following questions:

What is the priority of this risk? Use the prioritized list identified during the risk assessment process to decide how to allocate resources among the various control activities needed to reduce significant risks.

What is the cause of the risk? Consider reasons why the risk exists to identify control activities that could mitigate the risk.

What is the cost of the control versus the cost of the unfavorable event? Compare the cost of the risk's impact with the cost of the control activities to select the most cost-effective choice.

The Green Book identifies a list of control activity categories for management to consider in response to risk. Although not an exhaustive list, the Green Book categories are reproduced here for reference purposes:

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

Section Three: Control Activities

- 2. Design Control Activities.** Control activities carry out management's response to identified risks. A sound internal control plan will combine both preventative and detective controls to mitigate risks, implemented through a variety of automated or manual methods.
- Preventative controls deter the occurrence of an undesirable event. Development involves anticipating potential problems and implementing ways to avoid them. Examples of preventative controls include segregation of duties, authorization, verification processes, and physical security over assets.
 - Detective controls identify undesirable events that do occur and alert managers to take corrective action promptly. Examples of detective controls include reconciliations, report reviews, and performance reviews.

Automated controls might include validity and edit checks, sequential prenumbering of documents, or logical access security. Manual controls may include activities such as independent review, exception monitoring, and reconciliations.

Management must specifically address Segregation of Duties

Special emphasis must be placed on the segregation of duties because it reduces the risk of mistakes and inappropriate actions. The fundamental premise for segregated duties asserts that no one individual should control or perform all key aspects of a transaction or event – also known as incompatible duties when performed by the same individual.

No one employee should have job functions in more than one of the following three categories of duties:

1. Custody of Assets. This involves having physical access to agency assets or exercising control over an asset. Asset examples include cash, accountable items, equipment, and supplies. Exercising control includes initiating a payment in the accounting system, setting up a new employee in the payroll system, placing an order for supplies, specifying where orders are to be delivered, and receiving purchases.
2. Recordkeeping. This duty refers to the accounting or record keeping function, such as entering financial information into the accounting system.

Section Three: Control Activities

3. Approval. This duty belongs to persons with authority and responsibility to have others initiate and enter transactions. It also may involve reconciling and reviewing transactions for validity and reasonableness; periodic reviews and reconciliation of existing assets to recorded amounts; and comparisons at regular intervals and actions to resolve differences.

Examples of incompatible duties include –

- Managing both the operation of and record keeping for the same activity.
 - Receiving cash or checks, preparing deposits, and reconciling deposits
 - Entering new vendors and paying invoices
 - Entering and approving expenses
- Managing custodial activities and record keeping for the same assets.
- Authorizing transactions and managing the custody or disposal of the related assets or records.
- Operating and programming a computer system.

Specific examples from the *Accounting and Uniform Compliance Guidelines for State and Quasi-Agencies*, chapter 2 include:

- Individuals responsible for data entry of payment vouchers should not be responsible for approving these documents.
- Individuals responsible for acknowledging the receipt of goods or services should also not be responsible for purchasing approvals or payment activities.
- Managers should review and approve payroll expenses and time sheets before data entry but should not be involved in preparing payroll transactions.
- Individuals performing physical inventory counts should not be involved in maintaining inventory records nor authorize withdrawals of items maintained in inventory.
- Individuals receiving cash into the office should not be involved in recording bank deposits in the accounting records.
- Individuals receiving revenue or making deposits should not be involved in reconciling the bank accounts.

Section Three: Control Activities

A special note for smaller agencies . . .

As an integral part of the control activity component, segregation of duties is expected.

In small agencies, segregation of duties may not be practical. In this case, compensating activities must 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. Document decisions to incorporate compensating controls to mitigate risks.

Management may consider going outside of the agency for help in implementing controls through the Centralized Accounting Division. The Centralized Accounting Division was established for small agencies to drive efficiencies by reducing overall state costs of back-office expenses because services are pooled using fewer employees and standardizes business processes across all business units. The Centralized Accounting Division provides various accounting functions, including accounts payable; accounts receivable; asset management; cashbook reconciliation; contract/grant agreement preparation and tracking through electronic signature process; general ledger; invoicing; payroll; payroll allocation; purchasing; project costing; federal draw; and travel arrangements. For more information, visit www.in.gov/sba/about-us/centralized-accounting/.

Management considers other types of Control Activities

While recognizing the expectation of segregation of duties, management must consider other types of control activities to address identified risks. When establishing control activities, consider all aspects of operations, including information technology systems and third-party service providers.

Section Three: Control Activities

Examples of Control Activities include –

Review and Approval. Approval indicates the confirmation of employee decisions, events, or transactions based on a review before the transaction takes place. Management should clearly document approval procedures and ensure employees obtain approvals in all required situations. For example, a manager reviews a purchase request from an employee to determine whether the expense is warranted. The manager's signature documents approval on the request.

Authorization. Authorization represents a control activity designed to ensure events or transactions are initiated and executed by those designated by management. Management should ensure that the conditions and terms of authorizations are clearly documented and communicated, and that significant transactions are approved and executed only by persons acting within the scope of their authority. For example, a manager may be authorized to approve purchase requests, but only up to a certain dollar amount.

Verification/Reconciliation. Verification enables management to ensure activities are being performed consistently in accordance with policies. Reconciliation compares two or more items to identify differences. Overall, verification and reconciliation processes confirm the completeness, accuracy, authenticity and/or validity of transactions, events, or information. Examples include:

- Reviewing vendor invoices for accuracy by comparing to purchase orders and contracts.
- Comparing cash receipts transactions to a cash receipts log and tracing to bank deposit records.
- Reviewing and verifying a participant's eligibility for State program services.
- Reconciling licenses issued to revenue received.

Supervision. Supervision describes ongoing oversight and guidance of an activity by designated employees to ensure the results of the control activity achieve established objectives. Supervisory responsibilities might include a duty to -

- Monitor, review, and approve the work of those performing the activity to ensure correctness.
- Provide guidance and training to minimize errors and ensure that employees understand management expectations.

Section Three: Control Activities

- Communicate duties and responsibilities assigned to those performing the activities.

Documentation. Documentation of policies and procedures critically impacts the daily operations of an agency. Standard operating procedures set forth the fundamental framework and the underlying methods and processes all employees rely on to do their jobs and form the basis for decisions.

Principle Eleven:
Management designs the information system and related control activities to achieve objectives and respond to risks.

- 3. Specifically Address the Information System.** The use of an IT system can create risks to the internal control structure. For example, the procedures and calculations performed by the IT system must be checked for proper functioning. 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 unauthorized use to avoid the recording of unauthorized transactions, unauthorized changes to existing data, or loss of data in the event of a failure of the IT system.

Information Technology controls support the completeness, accuracy, and validity of information processed; protect data and program integrity from error or malicious intent; and prevent unauthorized programs or inappropriate modifications to existing programs or files.

According to the *Accounting and Uniform Compliance Guidelines Manual for State and Quasi-Agencies*, management evaluates changes to systems and updates control activities. 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.

Section Three: Control Activities

- 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. Audit Trails allow for sufficient documentation to trace all transactions from the original source of entry into the system, through all system processes, 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.

The State uses many different Information technology (IT) systems. These systems are an integral part of the internal control system. For example, the PeopleSoft accounting system provides many different internal controls over the financial reporting process:

- Permissions allow only certain users to perform certain tasks.
- Segregation of duties occurs by requiring duties to be completed by different users.
- The automation of processes and calculations enhances the internal control system by preventing errors.

Section Three: Control Activities

- Authority to access different components of the software is limited to employees with duties specifically related to that component.
- User ID and password sharing between employees is prohibited.
- Restrictions limit the authority to correct or adjust records to key employees or management.

The Indiana Office of Technology (IOT) was created to consolidate IT organizations across Indiana state government. According to Indiana Code 4-13.1, IOT –

- Establishes the standards for the technology infrastructure of the state.
- Focuses state information technology services to improve service levels to citizens and lower the costs of providing information technology services.
- Brings the best and most appropriate technology solutions to bear on state technology applications.
- Improves and expand government services provided electronically.
- Provides for the technology and procedures for the state to do business with the greatest security possible.

For more information on IOT policies and services, visit www.in.gov/iot.

*Principle Twelve:
Management implements
control activities through
policies.*

- 4. Document Control Activities.** Control activities are deployed through policies that define responsibility for objectives, risks, and control activity design, implementation, and operating effectiveness. Standard operating procedures put those policies into action. Documentation may include written narratives and flowcharts. Policies must require a mechanism to provide tangible evidence that control activities were performed.
- 5. Communicate Responsibility.** To help employees understand how and when to perform assigned responsibilities, policies and standard operating procedures must be communicated and available to employees in accordance with their duties. Management must ensure employees understand their responsibilities related to policies affecting their functions, including the responsibility to investigate and act upon discrepancies. Communication methods might include newsletters, staff meetings, or webinars.

Section Three: Control Activities

- 6. Review Policies and Procedures.** Management should periodically review policies, standard operating procedures, and related control activities for relevance and effectiveness in achieving objectives and addressing related risks. Review processes may include having discussions with personnel at defined time intervals, identifying significant changes affecting internal control activities, or coordinating an independent review of the design.

Documenting Control Activities

Control Activities must be documented. Documenting the agency's internal control system fosters communication and understanding of the internal control system. Benefits encompass the capability to –

- Communicate the design, implementation, and operating effectiveness of the internal control system to personnel.
- Retain organizational knowledge and mitigate the risk of having knowledge limited to a few personnel.
- Support the results of ongoing monitoring, identify internal control issues, and support the appropriate corrective actions.
- Provide tangible audit evidence to internal and external assurance providers. As part of the audit engagement, auditors will ask for written internal controls, and test those controls to determine the nature, timing, and extent of audit testing. Written internal controls must incorporate a process to maintain tangible evidence that the controls are functioning as intended. For example, if an internal control states that eligibility will be verified in accordance with an agency checklist by Person B, auditors will need to review evidence that Person B performed the verification process.

Methods to document the internal control system include narratives, flowcharts, and standard operating procedures. Part Three contains optional tools to facilitate and document the evaluation and development of internal controls.

Uniform Compliance Guidelines on Internal Controls for State and Quasi Agencies

<p>Part Two: Evaluation and Development of the Agency Internal Control System</p> <p>Section Four: Information and Communication</p>	<p>Issue Date: April 11, 2024</p>
	<p>Revision Date:</p>

Table of Contents

Overview	71
Why It Matters	71-72
Where to Start	72-73
Developing Agency Information and Communication Processes	73-77
Identify Information Requirements	74
Gather Quality Data	75
Process the Information	75
Establish Internal Communication Pathways	75-76
Establish External Communication Channels	76-77
Documenting Agency Information and Communication Processes.....	77-78

Section Four: Information and Communication

Overview

Information and communication processes pervade all internal control components, making this component vital for an agency to achieve objectives. Quality information must be identified, captured, and communicated in a form and timeframe that enables people to carry out their responsibilities.

What is quality information? Quality information is relevant, reliable, and timely. High quality information must be conveyed both within the agency and to external parties.

Principles thirteen through fifteen apply to the Information and Communication component.

Principle Thirteen: Management uses quality information to achieve agency objectives.

Principle Fourteen: Management internally communicates the necessary quality information to achieve agency objectives.

Principle Fifteen: Management externally communicates the necessary quality information to achieve agency objectives.

Why It Matters

All aspects of a strong internal control system rely on quality information and effective communication methods.

Information is necessary to carry out internal control responsibilities and support the achievement of objectives, such as:

- Providing essential data and high-quality information for informed decision making.
- Facilitating efficient operations, cost savings, and improved productivity through streamlined communication processes.
- Promoting transparency and confidence in agency operations through readily accessible and trustworthy information.
- Preventing fraud by identifying suspicious activities and restricting sensitive information.
- Supporting collaboration, knowledge sharing, and the achievement of common goals.
- Identifying areas for improvement.

Section Four: Information and Communication

The Information and Communication component of internal control contributes to the overall success of the State and each agency. It not only supports daily operations but also adds to risk management, compliance, and strategic planning, all of which are essential for achieving organizational objectives.

Where to Start

Evaluating agency information and communication processes serves as the optimal starting point for developing a successful internal control system. After evaluation, additional controls may be developed by following recommended steps or other processes determined by management. To be effective, the internal control system must be documented.

Evaluating Agency Information and Communication Processes

Does the agency have documented information and communication policies and procedures? Internal Control evaluation involves conducting periodic assessments of the agency's internal controls to determine whether,

- The agency will likely achieve its objectives.
- Risks to the agency and opportunities for improvement are identified.
- The elements of the agency's internal control system are functioning effectively.

Evaluation presents an opportunity to discuss and document internal controls. Meaningful and successful evaluations combine input from leadership across the agency, including major department or program areas. During this process, the consideration of absent controls will strengthen information and communication processes and facilitate an action plan for the design and implementation of a full-bodied internal control system.

Tools for Evaluation. Part Three contains an optional tool for management to use in the evaluation of agency information and communication processes. Management may choose this tool or consider other methods of evaluation based on the needs of the agency.

Section Four: Information and Communication

Information and Communication Internal Control Evaluation Template. This spreadsheet identifies common best practices for the information and communication component. A series of open-ended self-evaluation questions will guide management through major internal control considerations with the ability to designate current controls as sufficient, needing improvement, or nonexistent. [\[Link\]](#)

Based on the evaluation of information and communication processes, management may consider developing additional controls by following the recommended steps in "*Developing Agency Information and Communication Processes.*"

Developing Agency Information and Communication Processes

Quality information enables management to support the internal control system, determine risks, and communicate policies. To be effective for the achievement of objectives, information must be current, accurate, appropriate in content, and available on a timely basis at all staff levels.

Through the evaluation process, management may decide that internal controls need improvement.

A full-bodied internal control system addresses each internal control principle. The following steps, organized by principle, may be considered by management in the development of information and communication processes.

1. Identify Information Requirements
2. Gather Quality Data
3. Process the Information
4. Establish Internal Communication Pathways
5. Establish External Communication Channels

Tool for Development. Part Three contains optional tools for management to use in developing agency information and communication processes. Management may **choose one** tool or other method suitable for the agency's needs.

Control Development Questionnaire. This document walks through the steps outlined in "Developing Information and Communication Processes" with examples of information and communication processes, and space to document controls or reference standard operating procedures.

Section Four: Information and Communication

Control Development Template. This spreadsheet provides an abbreviated method for management to design information and communication processes to address specific risks identified through the risk assessment process. This template follows steps outlined in "Developing Agency Information and Communication Processes."

Example Objectives, Risks, Controls. This document provides examples of objectives, risks, and controls for major transaction areas. Lists are not intended to be exhaustive or applicable to all agencies. [\[Link\]](#)

Each major transaction area may include some or all the following examples –

- Example Objectives and Risks.
- Minimum Internal Control Standards per the Accounting and Uniform Compliance Guidelines Manual for State and Quasi Agencies.
- Example Key Controls.

Principle Thirteen:
Management uses quality information to achieve agency objectives.

- 1. Identify Information Requirements.** Information requirements consider the expectations of both internal and external users. When identifying information requirements, ask –

What information do we need to support the functioning of the internal control system and achievement of objectives?

As part of this process, management must identify the policies, procedures, data, and reports needed. Knowing agency objectives and related risks will help identify information needs. Information needed to support the functioning of the internal control system might include:

- Information needed for effective monitoring of events, activities, and transactions to allow prompt reaction. For example, managers need operational and financial data to evaluate performance and goals of accountability for effective and efficient use of resources.
- Operational information to determine whether programs comply with laws and regulations.
- Analytical information to help identify specific trends or actions needed.

Section Four: Information and Communication

- 2. Gather Quality Data.** Quality information allows management to make informed decisions, address risks, and evaluate performance. When considering information requirements, ask –

Where do I get this information?

How do I know it is accurate and reliable?

Quality information contains the following attributes: accessible/available, complete, accurate, correct, current, protected, retained, sufficient, timely, valid, and verifiable.

- 3. Process the Information.** Pertinent information must be processed in sufficient detail, in the right form, and in the appropriate time to enable employees to carry out their duties and responsibilities. Questions to ask might include –

Who needs this information?

Is this information presented in a way that is useful?

When is this information needed?

Examples of processed information include grant expenditure reports from accounting records or performance measures reports from statistical data.

Quality must be maintained to support the functioning of the internal control system and achievement of objectives. As part of this process, management should consider costs and benefits so that the nature, quantity, and precision of information communicated are commensurate with and support the achievement of objectives.

Principle Fourteen:
Management internally communicates the necessary quality information to achieve agency objectives.

- 4. Establish Internal Communication Pathways.** Internal communication channels information in all directions (across, up, and down the agency) to ensure employees, management, and leadership stay informed, resulting in coordinated, informed decision making. An agency must internally communicate information, including objectives and responsibilities for internal control, to support the functioning of all components of the internal control system.

Section Four: Information and Communication

Effective communication channels –

- provide timely information.
- address individual needs.
- inform employees of their duties and responsibilities.
- enable the reporting of sensitive matters.
- empower employees to provide suggestions for improvement.
- provide the information necessary for all employees to carry out their responsibilities effectively.
- help management evaluate the internal control system.
- convey top management's message on the importance of internal control responsibilities.

Examples of internal communication channels include –

- Microsoft Teams Meetings (or similar platform).
- Webinars.
- Dashboards.
- Newsletters.
- Emails.
- Policies and Standard Operating Procedures.
- Regular Staff Meetings.
- Inhouse Training Sessions.

Examples of quality information received and communicated through the agency may include job descriptions detailing internal control responsibilities; financial reports; and performance measures.

Principle Fifteen:
Management externally communicates the necessary quality information to achieve agency objectives.

- 5. Establish External Communication Channels.** External communication flows in two directions – enabling inbound communication of relevant external communication and providing outbound information to external parties in response to requirements and expectations.

Communication channels should receive information from external sources that will assist the agency with achieving its objectives. External Audit Reports, Hotlines, and Customer Surveys represent examples of external communication coming into the agency.

Section Four: Information and Communication

Communication channels from the agency to external receivers must provide information relevant to the requester's needs in the achievement of agency objectives. Examples of information going out from the agency include providing information to the public, federal grantor agencies, vendors, contractors, and subrecipients.

Conveying information externally involves many different layers of internal controls including the control environment, the risk assessment process, and control activities. Before information is released to an outside party, management must be confident about the accuracy of information, based on internal policies and procedures.

In establishing external communication channels, consider –

- Evaluating the reliability of information provided to and received from external parties.
- Ensuring only authorized individuals provide information to external parties.
- Safeguarding restricted information for authorized external parties.
- Communicating to employees the availability of separate reporting lines such as the Inspector General Hotline, or the State Board of Accounts Fraud Reporting Form.

Documenting Agency Information and Communication Processes

Information and Communication processes must be documented. Documenting the agency's internal control system fosters communication and understanding of the internal control system. Benefits encompass the capability to –

- Communicate the design, implementation, and operating effectiveness of the internal control system to personnel.
- Retain organizational knowledge and mitigate the risk of having knowledge limited to a few personnel.
- Support the results of ongoing monitoring, identify internal control issues, and support the appropriate corrective actions.

Section Four: Information and Communication

- Provide tangible audit evidence to internal and external assurance providers. As part of the audit engagement, auditors will ask for written internal controls, and test those controls to determine the nature, timing, and extent of audit testing. Written internal controls must incorporate a process to maintain tangible evidence that the controls are functioning as intended. For example, if eligibility for a service is based on the participant's income, auditors may review agency processes to identify, gather, and communicate suitable information to appropriate program and finance staff.

Methods to document the internal control system include narratives, flowcharts, and standard operating procedures. Part Three contains optional tools to facilitate and document the evaluation and development of internal controls.

Uniform Compliance Guidelines on Internal Controls for State and Quasi Agencies

<p>Part Two: Evaluation and Development of the Agency Internal Control System</p> <p>Section Five: Monitoring</p>	<p>Issue Date: April 11, 2024</p>
	<p>Revision Date:</p>

Table of Contents

Overview	81
Why It Matters	82
Where to Start	82-83
Developing Agency Monitoring Procedures	84-90
Define Key Controls	85
Establish a Baseline	86
Set Benchmarks	86
Select Monitoring Methods.....	86-88
Gather Information.....	88-89
Assess Monitoring Results	89
Implement Corrective Action	89-90
Documenting Monitoring Procedures	90-91

Section Five: Monitoring

Overview

How do I know that internal controls are working? By monitoring, or performing evaluations. Monitoring involves a process to select, develop, and perform ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning. Monitoring ensures that internal control aligns with changing objectives, environment, laws, resources, and risks.

Principles sixteen and seventeen apply to the monitoring component of internal control.

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

Principle Seventeen: Management remediates identified internal control deficiencies on a timely basis.

Monitoring activities and control activities can be easily confused. Many of the control activities can also be used as monitoring activities with the only difference being the intent of the control. For example,

- Reviewing a reconciliation for accuracy and supporting documents is a control activity; reviewing a reconciliation to ensure that appropriate personnel completed and reviewed the reconciliation in accordance with internal control procedures is a monitoring activity.
- Reviewing a purchase request to determine whether the expense is warranted is a control activity; reviewing a purchase request to see that proper authorization was given in accordance with agency policy is a monitoring activity.
- Reviewing program eligibility for a program participant is a control activity; reviewing participant eligibility to ensure eligibility requirements were applied correctly and documented in accordance with internal control procedures is a monitoring activity.

When considering monitoring activities, understanding the purpose of the activity will help avoid confusion.

As a fundamental aspect of maintaining strong internal controls, monitoring helps agencies adapt to evolving risks and challenges. Monitoring is most effective and efficient when the agency prioritizes and allocates resources based on the importance of the control to meeting the agency mission and core business objectives.

Section Five: Monitoring

Why It Matters

Controls left unmonitored tend to weaken with the passage of time. Monitoring, as defined in the COSO Internal Control Framework ensures "that internal control continues to operate effectively."

Effective design and implementation of monitoring leads to advantages for agencies by –

- Providing feedback for ongoing improvements in control systems and processes.
- Ensuring that an agency adheres to legal and regulatory requirements.
- Maintaining the integrity of financial information.
- Addressing weakness or vulnerability in agency operations, reducing risk.
- Determining whether enhancements to the internal control system are needed to ensure risks are continually mitigated to an acceptable level.
- Identifying improvements that can lead to cost savings and better resource allocation.
- Assessing the quality of performance over time.
- Resolving audit findings.
- Demonstrating a commitment to transparency and accountability.
- Streamlining the internal control assessment process.
- Providing a basis for annual internal control certification.

Over time, proactive monitoring can lead to enhanced organizational efficiency and cost reduction by identifying and addressing issues in advance, reducing the need for reactive measures.

Where to Start

Evaluating agency monitoring procedures serves as the optimal starting point for developing a successful internal control system. After evaluation, additional controls may be developed by following suggested steps in "*Developing Agency Monitoring Procedures*" or other processes determined by management. To be effective, the internal control system must be documented.

Section Five: Monitoring

Evaluating Agency Monitoring Procedures

Does the agency have documented monitoring policies and procedures? Internal Control evaluation involves conducting periodic assessments of the agency's internal controls to determine whether,

- The agency will likely achieve its objectives.
- Risks to the agency and opportunities for improvement are identified.
- The elements of the agency's internal control system are functioning effectively.

Evaluation presents an opportunity to discuss and document internal controls. Meaningful and successful evaluations combine input from leadership across the agency, including major department or program areas. During this process, the consideration of absent controls will strengthen monitoring procedures and facilitate an action plan for the design and implementation of a full-bodied internal control system.

Tools for Evaluation. Part Three contains an optional tool for management to use in the evaluation of agency monitoring procedures. Management may choose this tool or consider other methods of evaluation based on the needs of the agency.

Monitoring Internal Control Evaluation Template. This spreadsheet identifies common best practices for the monitoring component. A series of open-ended self-evaluation questions will guide management through major internal control considerations with the ability to designate current controls as sufficient, needing improvement, or nonexistent. [\[Link\]](#)

Based on the evaluation of monitoring procedures, management may consider developing additional controls by following the recommended steps in "*Developing Agency Monitoring Procedures.*"

Section Five: Monitoring

Developing Agency Monitoring Procedures

Monitoring internal controls involves a systematic process to determine whether controls in place are effective in achieving objectives.

A full-bodied internal control system addresses each internal control principle. The following steps, organized by principle, may be considered by management in the development of monitoring procedures.

1. Define Key Controls
2. Establish a Baseline
3. Set Benchmarks
4. Select Monitoring Methods
5. Gather Information
6. Assess Monitoring Results
7. Implement Corrective Action

Tool for Development. Part Three contains optional tools for management to use in developing agency monitoring procedures. Management may **choose one** tool or other method suitable for the agency's needs.

Control Development Questionnaire. This document walks through the steps outlined in "Developing Agency Monitoring Procedures" with examples of monitoring procedures and space for management to document answers for designing controls to suit the needs of the agency.

Control Development Template. This spreadsheet provides an abbreviated method for management to design monitoring procedures to address specific risks identified through the risk assessment process. This template follows steps outlined in "Developing Agency Monitoring Procedures."

Example Objectives, Risks, Controls. This document provides examples of objectives, risks, and controls for major transaction areas. Lists are not intended to be exhaustive or applicable to all agencies. [\[Link\]](#)

Each major transaction area may include some or all the following examples –

- Example Objectives and Risks.
- Minimum Internal Control Standards per the Accounting and Uniform Compliance Guidelines Manual for State and Quasi Agencies.
- Example Key Controls.

Section Five: Monitoring

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

- 1. Define Key Controls.** Monitoring is risk based, which enables evaluators to focus efforts on the key controls that address the most important risks. Key controls prevent or detect errors if all other controls fail. For example, controls which segregate duties for custody of assets, recordkeeping, and authorization are key controls.

When setting up monitoring activities, pinpoint key controls that mitigate significant risks. Key controls have one or both of the following characteristics:

- Operation of a key control prevents other control failures or detects such failures before they become material to the agency's objectives.
- Failure of a key control could materially affect the achievement of objectives and not be detected in a timely manner by other controls or monitoring procedures.

To get started, consider focusing monitoring efforts on –

- Key controls needed to resolve audit findings.
- Key controls to address the top risks identified by management.
- Significant changes to the agency's environment which may necessitate adjustments to internal controls.
-

Add other key controls in order of importance. Some factors to consider include:

- Size and Complexity, including complicated activities, regulatory requirements, services provided, sensitive transactions.
- Nature of Operations, including a high level of change in personnel, processes, or technology.
- Rate of Change, such as changes to programs or services provided, processes, and supporting technology.
- Importance of Controls to meeting agency mission and objectives.

Section Five: Monitoring

- 2. Establish A Baseline.** For key controls and risks identified, establish a baseline of known effective internal controls. This will be the foundation of ongoing monitoring and separate evaluations. Sources of baseline criteria include agency standard operating procedures, Accounting and Uniform Compliance Guidelines for State and Quasi Agencies, Financial Management Circulars, State policies and procedures, Indiana Code, Code of Federal Regulations, grantor requirements, best practices, and other authoritative sources.
- 3. Set Benchmarks.** Once key controls are selected and a baseline established, form clear benchmarks to evaluate the effectiveness of controls. Benchmarks should be measurable and specific. For example, specific and measurable criteria to evaluate the effectiveness of a cash receipts reconciliation to accountable items could include accuracy; timeliness to complete the reconciliation; timeliness of discrepancy resolution; and sufficiency of documentation. Through a comparison of the monitoring results to the established baseline, management can assess the quality of internal controls over time and adjust, as necessary.
- 4. Select Monitoring Methods.** Choose appropriate methods for monitoring. Monitoring may be performed on an ongoing basis and through separate evaluations to determine whether all five components of internal control are present and functioning.

Ongoing monitoring through day-to-day operations is the most timely and responsive to change. It occurs when the routine operations of the agency provide feedback through direct and indirect information to those responsible for the effectiveness of the internal control system. Examples include –

- Using automated tools.
- Performing regular management and supervisory activities.
- Preparing comparisons.
- Performing reconciliations.

Separate evaluations, apart from day-to-day operations, periodically assess whether controls effectively mitigate risks to an acceptable level. Separate evaluations vary in scope and frequency depending on risk assessment or results of ongoing evaluations. Examples include –

Section Five: Monitoring

- Self-assessments.
- Reviews by staff or management independent of the performance of key controls.
- Audit results and other evaluations.
- Data Analysis and trend monitoring.
- Tests and Sampling.

The following table provides insight on how to determine the appropriate monitoring approach and appropriate type of information to use when monitoring internal controls.

Importance of Control	Determining Factors	Possible Monitoring Approach
Highest	Controls that mitigate risks with high likelihood of occurring (frequency), and high impact (severity) to the department.	Ongoing monitoring activities using direct and indirect information, with periodic separate evaluations of direct information.
Moderate with short-term duration	Controls that mitigate risks with low likelihood of occurring (frequency), but high impact (severity) to the department.	Ongoing monitoring using indirect information, with periodic separate evaluations of direct information.
Moderate with long-term duration	Controls that mitigate risks with high likelihood of occurring (frequency), but low impact (severity) to the department.	Ongoing monitoring using indirect, with less-frequent, separate evaluations of direct information.
Lowest	Controls that mitigate risks with low likelihood of occurring (frequency), and low impact (severity) to the department.	Senior management may not monitor or may use infrequent separate evaluations.

Regardless of the method chosen, monitoring procedures will involve evaluators who are responsible for designing the monitoring activities, assessing monitoring results or information, and reaching conclusions regarding the effectiveness of internal control. Some evaluators may be responsible for overseeing processes or monitoring the operation of certain controls as part of their routine job functions.

Section Five: Monitoring

Evaluators must be knowledgeable about the internal control system, how controls should operate, and what constitutes a control deficiency. Objectivity is also a crucial factor, but its extent may vary depending on the type of monitoring being conducted. For example, self-review is the least objective, peer/coworker review is somewhat objective; supervisory review is more objective than peer review; and impartial review is the most objective (review by staff from other departments or external parties).

Through a strong control environment, management must educate all personnel about their role in monitoring internal controls and establish a system to report identified issues.

5. Gather Information. Working information and communication processes facilitate the gathering of information for monitoring purposes. Effective monitoring requires management to evaluate sufficient "suitable information." Suitable information is relevant, reliable, and timely. Information that meets these conditions is defined as "persuasive" within the COSO Guidance on Monitoring Internal Control Systems.

- *Relevant* data logically connects with the information requirements; the sources of data can be operational, financial, or compliance related. Relevant data impacts management's decision-making process or the achievement of objectives.
- *Reliable* data will be complete and accurate, free from error and bias.
- *Timely* data allows for effective decision-making and monitoring.

Monitoring can include both direct and indirect information.

- Direct information comes by observing controls in operation, reperforming them, or otherwise evaluating their operation directly to ensure the control was performed. For example, reperforming a bank reconciliation; reviewing expense documentation for proper authorization; or reviewing an eligibility determination.
- Indirect information may include operating statistics, key risk indicators, key performance indicators, and comparative industry metrics that may indicate a change or failure in the operation of controls. For example, a trend analysis showing an unusual decline in revenue received or an atypical increase in program expenses.

Section Five: Monitoring

The type of information gathered depends on the level of assurance desired. As part of the information gathering process, management will want to consider the desired level of assurance and methods needed to obtain that level of assurance. Examples include, from the least to the greatest level of assurance –

- Inquiries of appropriate personnel (inquiry alone is not sufficient support).
- Observations of operations.
- Inspections of relevant documentation.
- Reperformance of the application of a control (greatest level of assurance).

Principle Seventeen:
Management remediates identified internal control deficiencies on a timely basis.

6. Assess Monitoring Results. Monitoring will confirm the sufficiency of internal controls or identify shortcomings. By assessing monitoring results, management may identify ways to improve the efficiency of internal control or areas where change may provide a greater likelihood the agency will achieve its objectives.

When deficiencies have been identified internally, management must determine whether identified issues require further evaluation and remediation. For example, management may conduct a risk assessment and evaluate the residual risk for impact and likelihood.

If the residual risk adversely impacts the achievement of a statewide goal, the agency's mission or core business objectives, management must consider a plan for resolution. A cost-benefit analysis should also be performed to determine the appropriate level of action.

7. Implement Corrective Action. Internal control deficiencies may be identified internally through monitoring or externally through audit reports, communication from grantor agencies, and other similar sources. Management addresses deficiencies through the development of corrective action plans. Management and leadership work together to ensure the corrective action plan is implemented and the resulting changes are effective in correcting internal control weaknesses. As part of this process, management must –

- Ensure that corrective actions address the root causes of the issues. These corrective actions include the resolution of audit findings.

Section Five: Monitoring

- Communicate deficiencies to parties responsible for taking corrective action and persons identified in related policies and procedures.
- Delegate authority for completing corrective actions to appropriate personnel.
- Track corrective action plans to ensure deficiencies are remediated on a timely basis. Persons responsible for tracking corrective action should differ from those conducting the monitoring activities.
- Use the insights gained from monitoring to improve internal controls and processes. Update controls as necessary to address changing risks and circumstances.

Agency leadership must facilitate cooperation at all levels to develop comprehensive corrective action plans, including the following components:

- Specific action steps to correct the deficiency.
- Actions to address the root cause.
- Implementation time frames.
- Individual accountability for corrective action plan implementation.

Documenting Monitoring Procedures

Monitoring processes must be documented. Documenting the agency's internal control system fosters communication and understanding of the internal control system. Benefits encompass the capability to –

- Communicate the design, implementation, and operating effectiveness of the internal control system to personnel.
- Retain organizational knowledge and mitigate the risk of having knowledge limited to a few personnel.
- Support the results of ongoing monitoring, identify internal control issues, and support the appropriate corrective actions.

Section Five: Monitoring

- Provide tangible audit evidence to internal and external assurance providers. As part of the audit engagement, auditors will ask for written internal controls, and test those controls to determine the nature, timing, and extent of audit testing. Written internal controls must incorporate a process to maintain tangible evidence that the controls are functioning as intended. For example, auditors may review agency procedures for reconciliation of revenue received to permits issued. If standard operating procedures state that a supervisor will monthly review reconciliation of revenue collected to permits issued and document the review via email, then auditors will need to review the supervisor's email verifying the monthly review of reconciliations.

Methods to document the internal control system include narratives, flowcharts, and standard operating procedures. Part Three contains optional tools to facilitate and document the evaluation and development of internal controls.

Uniform Compliance Guidelines on Internal Controls for State and Quasi Agencies

Part Three: Tools for Evaluation and Development of the Agency Internal Control System	Issue Date: April 11, 2024
	Revision Date:

Table of Contents

Tools for Evaluation:

Tools for Evaluation Overview	95-97
Control Environment Evaluation Questionnaire	99-102
Internal Control Evaluation (ICE) Templates	
Instructions for ICE Templates	103-104
Control Environment ICE	105-106
Risk Assessment ICE	107-109
Control Activities ICE	110-116
Information and Communication ICE	117-118
Monitoring ICE	119

Tools for Development:

Tools for Development Overview with Links	121-122
---	---------

Examples

Examples Overview	123
Objectives, Risks, and Key Controls	124-154

Tools for Evaluation Overview

(Optional evaluation tools to be used in conjunction with Uniform Compliance Guidelines on Internal Controls for State and Quasi Agencies)

Tools and examples provided in this section may be used in conjunction with steps in the Uniform Compliance Guidelines on Internal Controls for State and Quasi Agencies. Management may modify these tools or use other methods as deemed appropriate to evaluate, develop, and document the internal control system.

Control Environment

The control environment forms the foundation for a strong internal control system. Because it includes the overall attitude and actions of management regarding internal controls, the control environment does not generally change with a given objective.

Management may **choose one** of the available tools or consider other methods of evaluation based on the needs of the agency.

Control Environment Self Evaluation Questionnaire. A series of self-evaluation questions will guide management through major internal control considerations in a "yes or no" format, which will help management determine which areas need further development. This section contains a copy of the questionnaire for reference. The questionnaire may be downloaded for agency use at this link: [\[Outside Link\]](#)

Control Environment Internal Control Evaluation Template. This spreadsheet identifies common best practices for the control environment. A series of open-ended self-evaluation questions will guide management through major internal control considerations with the ability to designate current controls as sufficient, needing improvement, or nonexistent. This section contains a copy of the spreadsheet for reference. The template may be downloaded for agency use at this link: [\[Outside Link\]](#)

In conjunction with either tool, management may refer to *Example Objectives, Risks, and Controls* for ideas on objectives and risks related to the control environment. [\[Link\]](#)

Based on the evaluation of the control environment, management may consider opportunities for improving the control environment. Suggested steps to develop the control environment are in "*Developing the Control Environment*" in Part Two, Section One: Control Environment.

Risk Assessment

A successful risk assessment prioritizes key activities and controls by combining input from leadership across the agency, including major department or program areas. After conducting a risk assessment, management may use the Internal Control Evaluation template to evaluate processes used and make improvements if necessary.

Tools for Evaluation Overview

(Continued)

Risk Assessment Internal Control Evaluation Template. This spreadsheet identifies common best practices for conducting a risk assessment. A series of open-ended self-evaluation questions will guide management through major internal control considerations with the ability to designate current controls as sufficient, needing improvement, or nonexistent. This section contains a copy of the spreadsheet for reference. The template may be downloaded for agency use at this link: [\[Outside Link\]](#)

In conjunction with the template, management may refer to *Example Objectives, Risks, and Controls* for ideas on related objectives, risks, and controls for major transaction areas. [\[Link\]](#)

Based on the evaluation of the risk assessment process, management may consider opportunities for improvement. Suggested steps to develop the risk assessment process are in "*Conducting a Risk Assessment*" in Part Two, Section Two: Risk Assessment.

Control Activities

Control activities are actions implemented through policies and procedures that prevent or detect identified risks to the achievement of objectives.

Control Activities Internal Control Evaluation Template. This spreadsheet identifies common best practices for control activities. A series of open-ended self-evaluation questions will guide management through major internal control considerations with the ability to designate current controls as sufficient, needing improvement, or nonexistent. This section contains a copy of the spreadsheet for reference. The template may be downloaded for agency use at this link: [\[Outside Link\]](#)

In conjunction with the template, management may refer to *Example Objectives, Risks, and Controls* for ideas on related objectives, risks, and controls for major transaction areas. [\[Link\]](#)

Based on the evaluation of control activities, management may consider opportunities for improvement. Suggested steps to develop control activities are in "*Developing Agency Control Activities*" in Part Two, Section Three: Control Activities.

Tools for Evaluation Overview

(Continued)

Information and Communication

All aspects of a strong internal control system rely on quality information and effective communication methods.

Information and Communication Internal Control Evaluation Template. This spreadsheet identifies common best practices for the information and communication component. A series of open-ended self-evaluation questions will guide management through major internal control considerations with the ability to designate current controls as sufficient, needing improvement, or nonexistent. This section contains a copy of the spreadsheet for reference. The template may be downloaded for agency use at this link: [\[Outside Link\]](#)

In conjunction with the template, management may refer to *Example Objectives, Risks, and Controls* for ideas on related objectives, risks, and controls for major transaction areas. [\[Link\]](#)

Based on the evaluation of information and communication processes, management may consider opportunities for improvement. Suggested steps to develop additional controls are in "*Developing Agency Information and Communication Processes*" in Part Two, Section Four: Information and Communication.

Monitoring

Monitoring ensures controls continue to operate effectively.

Monitoring Internal Control Evaluation Template. This spreadsheet identifies common best practices for the monitoring component. A series of open-ended self-evaluation questions will guide management through major internal control considerations with the ability to designate current controls as sufficient, needing improvement, or nonexistent. This section contains a copy of the spreadsheet for reference. The template may be downloaded for agency use at this link: [\[Outside Link\]](#)

In conjunction with the template, management may refer to *Example Objectives, Risks, and Controls* for ideas on related objectives, risks, and controls for major transaction areas. [\[Link\]](#)

Based on the evaluation of monitoring procedures, management may consider opportunities for improvement. Suggested steps to develop additional controls are in "*Developing Agency Monitoring Procedures*" in Part Two, Section Five: Monitoring.

Control Environment Evaluation Questionnaire

(An optional tool to be used in conjunction with Uniform Compliance Guidelines on Internal Controls for State and Quasi Agencies)

Agency _____

Date _____

Evaluator _____

This questionnaire contains a series of yes or no questions for consideration in management's evaluation of the control environment. The list is not considered exhaustive, but merely as a starting point for analysis. Not all questions will be applicable to all agencies. Management is encouraged to modify or add questions as needed. Based on the evaluation of the control environment, management may consider opportunities for improving the control environment. Suggested steps to develop the control environment are in "Developing the Control Environment" in the Control Environment section: [\[Link\]](#)

Yes | No | N/A

- | | | | | |
|-----|-----|-----|----|--|
| ___ | ___ | ___ | 1. | Are the State of Indiana Employee Handbook, the State Ethics Code, and other statewide policies emphasized to employees by management? |
| ___ | ___ | ___ | 2. | If applicable, is an agency code of conduct communicated prominently throughout the agency? |
| ___ | ___ | ___ | 3. | Is the agency code of conduct periodically updated and reviewed (i.e., the code of conduct reviewed on an annual basis)? |
| ___ | ___ | ___ | 4. | Does the agency have an anonymous and confidential Whistleblower policy for communicating and receiving information regarding fraud, errors in financial reporting and misrepresentation or false statements made by management? |
| ___ | ___ | ___ | 5. | Have transactions been executed in accordance with the agency code of conduct and approved written policies and procedures? |
| ___ | ___ | ___ | 6. | Does management analyze and document the knowledge and skills required to accomplish tasks? |
| ___ | ___ | ___ | 7. | Are job responsibilities formally documented and reviewed annually by management and other individuals in a position of influence over financial reporting? |
| ___ | ___ | ___ | 8. | Has management established overall objectives in the form of a mission statement, goals, or other written operating statement(s)? |

Control Environment Evaluation Questionnaire

(Continued)

Yes | No | N/A

- ___ ___ ___ 9. Have objectives been clearly communicated to all employees?
- ___ ___ ___ 10. Are objectives established for key areas (i.e., operations, financial reporting, compliance, etc.)?
- ___ ___ ___ 11. Are policies and procedures consistent with statutory authority?
- ___ ___ ___ 12. Are operations performed in accordance with statutes governing the public agency?
- ___ ___ ___ 13. Does senior management review financial results and performance measures regularly?
- ___ ___ ___ 14. Are unusual variances between budget and actual examined?
- ___ ___ ___ 15. Does the agency compare its actual performance with its goals and objectives?
- ___ ___ ___ 16. Does management follow-up on audit findings?
- ___ ___ ___ 17. Are written policies and procedures for all major areas periodically reviewed and approved by leadership and readily available for use by all employees?
- ___ ___ ___ 18. Is there an organizational chart that clearly defines the lines of authority and responsibility?
- ___ ___ ___ 19. Does senior management review and update the organizational structure of the agency?
- ___ ___ ___ 21. Is monitoring of the agency's operations adequate?
- ___ ___ ___ 22. Are specific limits established for certain types of transactions and delegations clearly communicated and understood by employees within the agency?
- ___ ___ ___ 23. Have specific lines of authority and responsibility been established to ensure compliance with Federal and State laws and regulations?
- ___ ___ ___ 24. Does management understand the concept and importance of internal controls, including division of responsibility?

Control Environment Evaluation Questionnaire

(Continued)

Yes | No | N/A

- ___ ___ ___ 25. Is the internal control structure supervised and reviewed by management to determine if it is operating as intended?
- ___ ___ ___ 26. Are responsibilities segregated so that no single employee controls all phases of a transaction?
- ___ ___ ___ 27. Are there adequate policies and procedures for authorization and approval of transactions at the appropriate level?
- ___ ___ ___ 28. Are sufficient training opportunities to improve competency and update employees on new policies and procedures available?
- ___ ___ ___ 29. If known areas of knowledge are limited, has help been enlisted from peers, auditors, or outside consultants to identify alternatives and suggest solutions?
- ___ ___ ___ 30. Have managers been provided with clear goals and direction from the governing body or top management?
- ___ ___ ___ 31. Is information (i.e., findings, recommendations, etc.) provided by external auditors considered and acted upon in a timely manner?
- ___ ___ ___ 32. Does management ensure compliance with the State's and/or agency's personnel policies and procedures concerning hiring, evaluating, promoting, compensating, and terminating employees?
- ___ ___ ___ 33. Are job descriptions (and other documents that define key position duties/requirements) current, accurate and understood?
- ___ ___ ___ 34. Are employees cross-trained to ensure the uninterrupted performance of personnel functions?
- ___ ___ ___ 35. Does the agency have mechanisms in place to anticipate, identify, and react to risks presented by changes in government, economic, industry, regulatory, operating, or other conditions that can affect the achievement of the agency's goals and objectives?
- ___ ___ ___ 36. Is risk identification incorporated into management's short-term and long-term forecasting and strategic planning?

Control Environment Evaluation Questionnaire
(Continued)

Opportunities for Improvement

Based on answers to self-evaluation questions, management should list improvements that must be made to ensure a sufficient control environment, focusing on key controls first.

Controls to be improved:

REFERENCE COPY

Internal Control Evaluation (ICE) Template Instructions

(ICE templates are optional tools to be used in conjunction with the Uniform Compliance Guidelines on Internal Controls for State and Quasi Agencies)

Introduction





Evaluating current agency controls serves as the optimal starting point for developing a successful internal control system. Meaningful and successful evaluations combine input from leadership across the agency, including major department or program areas.

The Internal Control Evaluation (ICE) template incorporates analysis of the internal control system with best practices. Through the evaluation process, management will decide whether internal controls are sufficient or need improvement. If desired, management may use the Control Development Template (CDT) as a guide for developing internal controls.

How to use the ICE template

Best Practice Statements and Questions to Ask. The Best Practice Statements relate to internal control principles and lead up to the Questions to Ask. The questions help management consider the degree to which the system is functioning. The best practice statements and questions to ask are meant to be a flexible starting point for the evaluation of internal control, not an exhaustive list. Management is encouraged to consider additional evaluation questions as needed.

Rating Columns. Management may rate the responses to the Best Practice Statements and Questions to Ask based on the following guidelines:

-  Green: Controls are effective
-  Yellow: Controls need improvement or improvement is in progress
-  Red: Controls are not effective
-  N/A: Controls are not applicable

What Controls are currently in place? If controls receive a green or yellow rating, management may use this column to document what controls are currently in place. This could include references to a standard operating procedure, narrative, flowchart, policy, web page, etc.

Internal Control Evaluation (ICE) Template Instructions (Continued)

Will controls be improved or implemented? If controls receive a yellow or red rating, management will need to decide if those controls will be improved (yellow) or implemented (red). Management will want to perform a risk assessment and cost-benefit analysis to make this determination.

If no, document reason. Management may refer to the risk assessment, cost-benefit analysis, or other information used to determine controls will not be improved or implemented.

If yes, how will this be accomplished? Management will need to consider steps to develop the control. Management may use the control development tool to document the process, or other desired method to document management's plan.

Responsible Person. Management should delegate responsibility to ensure implementation in accordance with management's plan.

Target Completion Date. Management should set a goal for implementation.

Documentation

A copy of the completed ICE, along with any supporting control documentation should be organized and retained electronically. Organizing this information in a logical manner will provide easy access for future updates, revisions, and handling requests from internal or external parties, such as internal or external auditors.

Documentation will vary by agency. The amount of documentation gathered to evidence this evaluation depends on an agency's size, complexity of organizational structure and business activities. Actual documentation may include mission statements, goals, objectives, organization charts, policies, and procedures, etc.

Control Environment Internal Control Evaluation (ICE) Template

(an optional tool to be used in conjunction with the Uniform Compliance Guidelines on Internal Controls for State and Quasi Agencies)

Agency: _____

Evaluator: _____

Date of Evaluation: _____

Control Environment											
					Will controls be improved or implemented? (yellow or red status)						
Best Practice Statements	Questions to Ask				N/A	What controls are currently in place?(green/yellow status). Describe or Reference SOP	Yes	If no, document reason.	If yes, will the development of controls be documented on the Control Development Tool or other method (describe)?	Responsible Person	Target Completion Date
Principle One: The agency demonstrates a commitment to integrity and ethical values.											
Agency leadership has established a "tone at the top" that has been communicated to and is practiced by executives and management throughout the agency.	Are the Agency mission, goals and objectives effectively communicated to all employees? Where are these principles located? How often are these principles reemphasized to the employees (e.g., annually)?										
Management enforces a formal code or codes of conduct communicating appropriate ethical and moral behavioral standards through policy/training and addresses acceptable operational practices and conflicts of interest. Appropriate disciplinary action is taken in response to departures from such.	Is the State Ethics Code emphasized as an important part of the internal control system? Does the Agency have additional expectations for integrity and ethical values, such as an agency code of conduct? How are the state ethics code and other expectations communicated to employees? Where are they maintained? How are they enforced?										
Principle Two: Agency leadership oversees the internal control system.											
Agency leadership oversees the design, implementation, operation, and continued monitoring of Internal Controls.	Does leadership oversee management's design, implementation, and operation of the internal control system, including the monitoring of internal controls? Who in agency leadership provides oversight of the internal control system?										
Agency leadership independently reviews and discusses the internal control system, emphasizes continuous improvement and resolution.	How often does leadership review and discuss the internal controls? Is the Certification of Internal Controls completed per the requirements of FMC 6.1? Does leadership ensure that risk self-assessment questions are answered timely and accurately when requested by OMB? Does leadership monitor progress on resolution of internal control audit findings?										
Management takes appropriate action when controls are overridden and/or when exceptions to policies and procedures occur. Management reports deficiencies in internal controls to agency leadership.	Is a system in place to identify exceptions to the policies/procedures and how are they resolved? How does management report internal control deficiencies to leadership?										
Principle Three: Management establishes an organizational structure, assigns responsibility, and delegates authority to achieve agency objectives.											
Management has an up-to-date organizational chart which defines the lines of management authority/ responsibility and is shared with employees.	Is the agency structure documented in an organizational chart which defines the lines of management authority/responsibility? Is this organization chart explained and shared with employees?										
Management appropriately assigns authority and delegates responsibility to the proper personnel to deal with organizational goals and objectives.	How is each employee trained to understand their duties and authorities?										

Control Environment

Control Environment					Will controls be improved or implemented? (yellow or red status)						
Best Practice Statements	Questions to Ask	★	▲	●	N/A	What controls are currently in place?(green/yellow status). Describe or Reference SOP	Yes	If no, document reason.	If yes, will the development of controls be documented on the Control Development Tool or other method (describe)?	Responsible Person	Target Completion Date
Management appropriately documents its internal control system. Documentation is required to demonstrate the design, implementation, and operating effectiveness of the internal control system.	How has management documented its internal controls? How does management ensure the controls are implemented and operating as intended?										
Principle Four: Management demonstrates a commitment to attract, develop, and retain competent individuals.											
Management performs required personnel actions including the hiring of most qualified individuals based on skills, knowledge and experience, evidence of integrity and ethical behavior; and performing checks on background, credentials and references of new employees.	When hiring new employees, how does the Agency ensure the most qualified candidates are selected? Are references checked? Are background checks performed? How is this documented?										
Management has identified and defined the tasks required to accomplish particular jobs and fill various positions.	Are meetings held with management to review organizational needs and ensure necessary positions are filled, and additional positions are created when needed? Are job descriptions maintained and reviewed annually with all employees?										
Employees receive/obtain information and training about internal controls, as it pertains to one's position, role, and responsibilities to maintain and improve their competence for their jobs and enable each employee to contribute effectively to maintaining an effective internal control system.	Is training provided to maintain and improve employee competency and enable each employee to contribute effectively to maintaining an effective internal control system? If yes, how often does this training occur?										
Management utilizes methods such as cross-training, strategic hiring practices, detailed procedure documentation, enhanced supervision, etc. to help mitigate the risk associated with sudden or significant changes in key personnel.	Do detailed procedures or policies exist to cross-train employees or transition other employees into key roles in case of sudden changes in key personnel?										
Principle Five: Management evaluates performance and holds individuals accountable for their internal control responsibilities.											
Management enforces accountability of all individuals, including all agency personnel as well as all service organizations, by designating their internal control responsibilities, including responsibilities related to compliance with laws and regulations.	Does management enforce accountability of all individuals and service organizations by designating internal control responsibilities, including responsibilities related to compliance with laws and regulations?										
Job performance is periodically evaluated and reviewed with each employee. Appropriate remedial action is taken when performance expectations are not met. Inappropriate behavior is consistently reprimanded in a timely and direct manner, regardless of the individual's position or status.	Does the agency enforce accountability with respect to management, staff, and contractors? Are performance evaluations being conducted on a timely basis to ensure job duties (i.e. reconciliations, reviews) are being performed? What remedial actions are taken when performance is not adequate or inappropriate behavior is reported?										
Excessive pressure on employees is evaluated to ensure they are able to fulfill their assigned responsibilities. Excessive pressures are adjusted by rebalancing workloads, increasing resource levels, or by other methods.	Is excessive pressure placed on management, staff, contractors, etc. to complete tasks and/or their assigned duties? If yes, how do you protect against the related risks of corners being cut, quality diminishing, etc.?										

Risk Assessment Internal Control Evaluation (ICE) Template

(an optional tool to be used in conjunction with the Uniform Compliance Guidelines on Internal Controls for State and Quasi Agencies)

Agency _____

Evaluator: _____




Date of Evaluation: _____

Risk Assessment											
					Will controls be improved or implemented? (yellow or red status)						
Best Practice Statements	Questions to Ask				N/A	What controls are currently in place?(green/yellow status). Describe or Reference SOP	Yes	If no, document reason.	If yes, how will this be accomplished?	Responsible Person	Target Completion Date
Principle Six: Management defines objectives clearly to enable the identification of risks and defines risk tolerances.											
Agency has a defined strategic plan, including a mission statement and defined goals and objectives. The Agency plan identifies critical success factors and risks, including fraud risk, related to achieving the defined objectives. Measurement criteria are used to regularly assess whether agency objectives are achieved and identify new risks. Management has established a process to periodically review and update strategic plans and objectives.	Does the Agency define objectives, addressing critical success factors and risks related to goals and objectives? What measurement criteria is used to evaluate whether objectives are achieved and evaluate any new risks? What is the process for periodically reviewing and updating objectives?										
Management defines risk tolerances for its defined objectives in specific and measurable terms. This includes having specific measures in place to define what is a reasonable level of variation in performance in operational objectives, a reasonable level of precision and accuracy for nonfinancial reporting objectives, and a reasonable level of materiality for financial reporting objectives. Acceptable levels of variation are documented.	How does management define its risk tolerance for objectives? Does the Agency have a specific measure in place to define what is a reasonable level of variation in performance in operation objectives? Is there a specific measure in place to define what a reasonable level of precision and accuracy are for non-financial reporting objectives? Does the Agency have a specific measure in place to define a reasonable level of materiality to be used in making decisions regarding financial reporting objectives?										
Principle Seven: Management identifies, analyzes, and responds to risks related to achieving the defined objectives.											
A process exists to identify and consider the implications of internal risk factors (new personnel, new information systems, changes in management responsibilities, new or changed educational or research programs, etc.) on agency objectives and plans. This process is updated at least annually.	Does a process exist to identify and consider the implications of internal risk factors on objectives and plans? If yes, what is the process? How often is the process updated?										
A process exists to identify and consider the implications of external risk factors (new legislation, technological advancements, expectations of the federal government, etc.) on agency objectives and plans. This process is updated at least annually.	Does a process exist to identify and consider the implications of external risk factors on objectives and plans? How often is the process updated?										
Management has developed an approach for risk management that assesses the likelihood, frequency, and impact of each identified risk event; assigns a risk category (high, medium, low) to each event; and considers the costs versus the benefits of reducing the risk.	Does the Agency conduct a risk assessment of business processes? If so, how and when is it conducted?										

Risk Assessment

Risk Assessment					Will controls be improved or implemented? (yellow or red status)						
					Yes	If no, document reason.	If yes, how will this be accomplished?	Responsible Person	Target Completion Date		
Best Practice Statements	Questions to Ask	★	▲	○	N/A	What controls are currently in place?(green/yellow status). Describe or Reference SOP	Yes	If no, document reason.	If yes, how will this be accomplished?	Responsible Person	Target Completion Date
Senior management develops and documents its plans to mitigate significant identified risks by mapping risks to control activities.	Are plans developed and documented to mitigate significant identified risks? Are risks mapped to specific control activities?										
Management periodically assesses employee attitudes towards their specific roles in the agency, reviews the effectiveness of the organization structure, and evaluates the appropriateness of policies and procedures.	Is management open to feedback from employees and does management continually assess employee attitudes towards their roles (i.e. open-door policy)?										
Risk assessments are conducted on a regular basis. Management periodically evaluates the effectiveness of its risk assessment process which includes: 1) following up on control gaps and/or redundancies identified through the risk assessment process, taking corrective action to develop and/or strengthen internal controls, holding responsible parties accountable, and communicating action plan/status updates to management. 2) allocating resources to those areas of risk where the combination of risk likelihood and impact will sustain the greatest negative consequences.	Are risk assessments conducted on a regular basis? How does management periodically evaluate the effectiveness of its risk assessment process; including : 1) following up on control gaps and/or redundancies identified through the risk assessment process, taking corrective action to develop and/or strengthen internal controls, holding responsible parties accountable, and communicating action plan/status updates to management; and, 2) allocating resources to those areas of risk where the combination of risk likelihood and impact will sustain the greatest negative consequences?										
Management has an appropriate attitude toward risk taking and proceeds with new ventures, missions, or operations only after carefully analyzing the risks involved and determining how they may be minimized or mitigated.	How does management analyze risk before proceeding with any new venture, mission, or operation? How is this process documented?										
Principle Eight: Management considers the potential for fraud when identifying, analyzing, and responding to risks.											
Specific antifraud policies and training have been developed; periodically, employees receive training on fraud awareness and appropriate actions to take when fraud is suspected. Management has a fraud response plan in place and knows how to respond timely if a fraud allegation is made.	Does the Agency have specific internal antifraud policies. Has training been developed? If yes, is there a required periodic training for each employee to complete and sign off on? What is management's internal fraud response plan? Does management respond timely if an internal fraud allegation is made?										
Management performs fraud risk assessments on a regular basis to identify types of fraud that may be occurring (i.e. fraudulent financial reporting, misappropriation of assets, corruption). Management identifies fraud risk factors (incentive/pressure, opportunity, and attitude/rationalization) that often lead to fraud being committed. Also, management identifies other forms of misconduct that can occur such as waste and abuse. The assessment considers how to remedy control deficiencies identified.	How does management perform fraud risk assessments on a regular basis to identify types of fraud that may be occurring (e.g., review segregation of duties and cash controls to ensure that misappropriation of assets is not occurring)? How does management identify fraud risk factors? How does management consider other forms of misconduct such as waste and abuse?										
Management appropriately responds to identified fraud risk factors to mitigate the potential for fraudulent activity to occur.	How does management respond to any identified fraud risk factors (e.g., implement compensating controls to deter fraud)? How are identified fraud risk factors communicated to employees?										

Risk Assessment

Risk Assessment					Will controls be improved or implemented? (yellow or red status)					
					Yes	If no, document reason.	If yes, how will this be accomplished?	Responsible Person	Target Completion Date	
Best Practice Statements	Questions to Ask				N/A	What controls are currently in place?(green/yellow status). Describe or Reference SOP				
Principle Nine: Management identifies, analyzes, and responds to significant changes that could impact the internal control system.										
Management reviews risk assessments and identifies changes that need to be implemented to ensure controls will continue to operate efficiently and effectively. Management forecasts potential internal and external conditions that could change in the future, and communicates effectively to appropriate personnel.	How does management review risk assessments and identify changes needed to ensure controls will continue to operate efficiently and effectively? Does management forecast potential internal and external conditions that could change in the future and communicate these conditions to appropriate personnel?									
Mechanisms exist to identify, prioritize, and react to 1) routine events (i.e. turnover), 2) economic change, 3) regulatory changes, and 4) technological changes that impact the achievement of agency objectives	How does the Agency identify, prioritize, and react to routine events, economic change, regulatory changes, new legislation, and technological changes? How does management ensure that none of these changes are overlooked?									
Management promotes continuous improvement and solicits input and feedback on the implications of significant change.	Does management promote continuous improvement and solicit input and feedback on the implications of significant change? If yes, how does management evaluate input and promote continuous improvement?									

Control Activities Internal Control Evaluation (ICE) Template

(an optional tool to be used in conjunction with the Uniform Compliance Guidelines on Internal Controls for State and Quasi Agencies)

Agency: _____

Evaluator: _____

Date of Evaluation: _____

Control Activities						Will controls be improved or implemented? (yellow or red status)					
Best Practice Statements	Questions to Ask	★	▲	●	N/A	What controls are currently in place? (green/yellow status) Describe or Reference SOP	Yes	If no, document reason.	If yes, how will this be accomplished?	Responsible Person	Target Completion Date
Principle Ten: Management designs control activities to achieve objectives and respond to risks.											
Policies, procedures, techniques and/or mechanisms are in place to enforce management's directives to achieve the agency's objectives and address related risks.	Does the Agency have policies, procedures, techniques and/or mechanisms in place to enforce management's directives to achieve objectives and address related risks? Are policies and procedures designed to provide compliance with applicable laws, criteria, standards, uniform compliance guidelines and other requirements?										
Policies and procedures address the handling of confidential or sensitive information.	Does the Agency have policies and procedures in place to address the handling of confidential or sensitive information?										
Management has defined and appropriately assigned employee job duties, roles and responsibilities to qualified personnel to achieve agency objectives.	Has the Agency defined and appropriately assigned employee job duties, roles and responsibilities to qualified personnel to achieve control objectives?										
The agency has established and monitors performance measures and indicators.	Are performance measures monitored?										
Key duties and responsibilities are divided or segregated among different people to reduce the risk of error, waste, or fraud. For example, no one person should initiate transactions, reconcile balances, handle assets and review reports. If adequate segregation of duties is not practical, management has designed compensating control activities (i.e. additional supervision and review) to address the risk.	Does the Agency have a process in place to ensure adequate segregation of duties? If there are exceptions (i.e. instances where segregation of duties is not practical due to resource constraints), have compensating controls been implemented and documented to address the associated risks?										
Security and Data Access policies and procedures are in place to ensure timely review of user accounts and roles they are assigned within IT systems. The security and data policy should include access control, user provisioning, etc. At a minimum, an annual review of roles should be performed by management to ensure proper segregation of duties within IT systems.	Has the Agency implemented IT security and data access policies and procedures to ensure timely review of user accounts and roles assigned to your IT systems? Do the procedures implemented include access control, user provisioning, etc. Are roles reviewed at least annually to ensure proper segregation of duties within your IT systems?										
Management designs controls activities to ensure certain transactions need appropriate levels of review based on predetermined criteria set by management in response to determined risks.	Are dollar thresholds established to escalate transactions to a higher level of management for review/approval?										

Control Activities										
Best Practice Statements	Questions to Ask	★	▲	●	N/A	What controls are currently in place? (green/yellow status) Describe or Reference SOP	Will controls be improved or implemented? (yellow or red status)			Target Completion Date
							Yes	If no, document reason.	If yes, how will this be accomplished?	
Accounting reports and key reconciliations are completed timely. (i.e. reconciliation of grant expenditures is prepared and reviewed, purchasing card reconciliations) Management performs a diligent review and signifies approval by signature and date. Unexpected operating results or unusual trends are investigated.	Are accounting reports and reconciliations completed timely, documented, and reviewed and approved (evidenced by signatures and dates of those responsible)? Are anomalies investigated?									
Management designs appropriate types of control activities to address risks surrounding their control objectives. Management will take into consideration the following controls when designing effective control procedures: <ul style="list-style-type: none"> •Top Level Reviews of performance •Management of Human Capital •Controls over information processing (i.e. edit checks of data entered; accounting for transactions in numerical sequences; batch total with control accounts, etc.) •Physical control over vulnerable assets •Appropriate documentation (formal policies, directives, and manuals are properly managed and maintained) 	Does management utilize the appropriate type of control activities needed to address risks? Is access to state agency assets limited to authorized persons who require these assets in the performance of assigned duties?									
Management designs controls at the appropriate levels in response to risks identified. Management will incorporate transactional/activity controls (i.e. reconciliations, authorizations, etc.) into the operational process when necessary depending on the relevance of the transaction cycle in meeting the overall objective.	Does management design controls at the appropriate level in response to risks identified? Has management incorporated transactional/activity controls depending on the relevance of the transaction cycle in meeting the overall Agency control objective?									
Employees understand which records they are responsible to maintain and the required retention period. Records are appropriately filed and are disposed of according to the updated retention schedule.	How does management ensure that employees are aware of record retention policies and that records are appropriately maintained and disposed of according to the retention schedule?									
Management has a written policy in place which defines the procedures for monitoring sub-recipients: 1) The agency documents its review of sub-recipients. 2) The agency reviews corrective action plans of sub-recipients and follows up on past exceptions in future monitoring.	Does management have a written policy in place which defines the procedures for monitoring sub-recipients? Does management document its review of sub-recipients? Does management review corrective action plans of sub-recipients and follow up on past exceptions in future monitoring?									
Management confirms the operating effectiveness of service providers controls. Management inventories existing outsourced vendor relationships and assesses the impact of these outsourced services on their internal control environment. Management determines whether examinations, audits, service level agreements, and related independent reports are required as part of the contract with the third party service provider.	Does management confirm the operating effectiveness of their service providers' controls? Does management inventory existing outsourced vendor relationships and assesses the impact of these outsourced services on the internal control environment? Does management determine whether examinations, audits, service level agreements, and related independent reports should be required as part of the contract with the third-party service provider?									

Control Activities											
					Will controls be improved or implemented? (yellow or red status)						
Best Practice Statements	Questions to Ask	☆	△	●	N/A	What controls are currently in place? (green/yellow status) Describe or Reference SOP	Yes	If no, document reason.	If yes, how will this be accomplished?	Responsible Person	Target Completion Date
Management obtains and reviews all independent reports to ensure the independent report covers controls related to risks identified through vendor relationships and follows up on any areas of concern/deficiencies identified in the reports.	Does management obtain and review all independent reports to ensure the independent report covers controls related to risks identified through vendor relationships and follow up on any areas of concern/deficiencies identified in the reports?										
Principle Eleven: Management designs the information system and related control activities to achieve objectives and respond to risks.											
Access to Programs and Data											
Management designs the information system and use of the information technology by considering the requirements for operational processes. Management classifies information resources according to their criticality and sensitivity as they relate to objectives and risks.	Does management design the information system and use of the information technology by considering the requirements for operational processes? How does management know the technology infrastructure supports the completeness, accuracy, and validity of information processed? Does management classify information resources according to their criticality and sensitivity as they relate to Agency objectives and risks?										
Information Security Policy/User Awareness: 1) Information security policies and procedures are documented, and include user security administration, password management, login requirements, data security, privacy, and e-mail usage. 2) Information security policies are disseminated to all users.	Are information security policies and procedures documented, and do they include user security administration, password management, login requirements, data security, privacy, and e-mail usage? Are information security policies disseminated to all users?										
Application settings are in place to control access to systems through password parameter settings.	Are application settings in place to control access to systems through password parameter settings?										
Access Administration: 1) Network and application access requests for new employees are communicated to the system administrators. Upon receiving notification, the member of this group will grant access based upon job responsibilities. 2) When an employee separates from employment, system administrators are notified. Upon notification the system administrator suspends the user's ID on the employee's last day. 3) Administrative access to the network and applications is restricted to individuals in the IT group who have been appropriately authorized by management and require this level of access to perform their job function.	Access Administration: 1) Are network and application access requests for new employees communicated to the system administrators? Upon receiving notification, does the member of this group grant access based upon job responsibilities? 2) When an employee separates from employment; are system administrators notified? Upon notification, do the system administrator suspend the user's ID on the employee's termination date? 3) Is administrative access to the network and applications restricted to individuals in the IT group who have been appropriately authorized by management and require this level of access to perform their job function?										
In order to access application functionality, users must authenticate through the network using a unique user ID and password.	In order to access application functionality, do users have to authenticate through the network using a unique user ID and password?										





Control Activities										
Best Practice Statements	Questions to Ask	☆	△	●	N/A	What controls are currently in place? (green/yellow status) Describe or Reference SOP	Will controls be improved or implemented? (yellow or red status)			Target Completion Date
							Yes	If no, document reason.	If yes, how will this be accomplished?	
On a regular basis management performs an access review of all users. Managers verify that access is commensurate with users' job function. A restricted group performs all modifications to information system access.	Does management perform an access review of all users on a regular basis? Are managers required to verify that access is commensurate with users' job function? Is a restricted group responsible for granting, changing, and removing access to information systems?									
Privileged Access: 1) Access to special privileges (i.e., Security, Super) within applications is limited to personnel authorized by management. 2) Administrative access to the operating system/servers is limited to authorized personnel. 3) Administrative and privileged access (write/execute) to databases is limited to authorized personnel.	Privileged Access: 1) Is access to special privileges within applications limited to personnel authorized by management? 2) Is administrative access to the operating system/servers limited to authorized personnel? 3) Is administrative and privileged access (write/execute) to databases limited to authorized personnel? Is activity logged and monitored?									
Physical Access: 1) Access to the system is restricted so that only individuals who need access to perform their daily job responsibilities have access. Access Logs are reviewed to ensure no unauthorized personnel were admitted. 2) The software functions are password protected and only the administrator and designated backups have access to the system.	Physical Access: 1) Is access to the system area restricted? How is access restricted? Are only those individuals who need access to perform their daily job responsibilities able to access? Are access logs reviewed? 2) Are software functions password protected and do only the administrator and designated backups have access to the system?									
Firewalls, intrusion prevention systems and spam filters are in place at the perimeter of the network to reduce the risk of unauthorized access. Management periodically monitors reports/logs to identify potential unauthorized activity.	Are firewalls, intrusion prevention systems and spam filters in place to reduce the risk of unauthorized access? Does management periodically monitor reports/logs to identify potential unauthorized activity?									
Program Changes										
Written systems and programming standards are established to outline requirements for changes to application software, system patching, configuration changes, and emergency changes.	Have written systems and programming standards been established to outline requirements for changes to application software, system patching, configuration changes, and emergency changes?									
Management authorization is requested and obtained prior to initiating an application change.	Is management authorization requested and obtained prior to initiating an application change?									
Application changes are tested, and results of successful testing are documented prior to implementation.	Are application changes tested, and are results of successful testing documented prior to implementation?									
Management approval is requested and obtained prior to final implementation of an application change. Approval for emergency changes is documented by management.	Is management approval requested and obtained prior to final implementation of an application change? Is approval for emergency changes documented by management?									

Control Activities

Control Activities					Will controls be improved or implemented? (yellow or red status)						
Best Practice Statements	Questions to Ask	★	▲	●	N/A	What controls are currently in place? (green/yellow status) Describe or Reference SOP	Yes	If no, document reason.	If yes, how will this be accomplished?	Responsible Person	Target Completion Date
Administrative access required to implement system software changes into the production environment is restricted to authorized personnel who require such access to perform job duties. Developers and end users do not have the administrative access required to implement system software changes into the production environment. Shared/system user IDs do not exist and/or the implementation of changes is performed through the use of a scheduled job. Release notices are sent to IT staff and business units as required.	Is administrative access required to implement system software changes into the production environment and is this access restricted to authorized personnel who require such access to perform job duties? How does management ensure that developers and end users do not have the administrative access required to implement system software changes into the production environment? How does management ensure that shared/system user IDs do not exist? Are release notices sent to IT staff and business units as required?										
Program Development											
A written system development lifecycle is established to outline requirements for planning, designing, developing, testing, approving, and implementing new applications and upgrades to existing applications, including vendor-developed software.	Has a written system development lifecycle been established to outline requirements for planning, designing, developing, testing, approving, and implementing new applications and upgrades to existing applications, including vendor-developed software?										
For all new applications or upgrades, appropriate project management documentation is prepared to define project scope, requirements, project plans, and milestones.	Is appropriate project management documentation prepared for all new applications or upgrades? Does this documentation define the project scope, requirements, project plans, and milestones?										
Management authorization is documented for all system implementations and upgrades. For all new application development efforts, a detailed design is established based on business requirements and considers all objectives, including functionality and security during and after development. Developers do not have access to modify final production code during and after system implementations.	Is management authorization documented for all system implementations and upgrades? Is a detailed design established for all new application development efforts? Is the design based on business requirements and does it consider all objectives, including functionality and security during and after development? How does the unit ensure that developers do not have access to modify final production code during and after system implementations?										
For all new or upgraded applications, testing is planned and results of successful testing by IT, software vendors (if applicable), and user groups are documented prior to implementation.	Is testing planned for all new or upgraded applications? Are results of successful testing by IT, software vendors (if applicable), and user groups documented prior to implementation?										
Management approval is requested and obtained prior to final implementation of a new or upgraded application. Approval is documented.	Is management approval requested and obtained prior to final implementation of a new or upgraded application? Is approval documented?										
The implementation of new and upgraded application software is documented, and supporting system documentation is established and retained. If data migration is performed as a result of the new/upgraded application software, reconciliations are performed to ensure that data migrated successfully and accurately. Support for reconciliations is retained. A post-implementation review for all new or upgraded application software is performed by IT, end users, and software vendors (if applicable) to ensure that the system is functioning correctly in the production environment.	Is the implementation of new and upgraded application software documented, and is supporting system documentation established and retained? If data migration is performed as a result of the new/upgraded application software, are reconciliations performed to ensure that data migrated successfully and accurately? Is support for reconciliations retained? Is a post-implementation review for all new or upgraded application software performed by IT, end users, and software vendors (if applicable) to ensure that the system is functioning correctly in the production environment?										

Control Activities

Control Activities						Will controls be improved or implemented? (yellow or red status)				
Best Practice Statements	Questions to Ask		N/A	What controls are currently in place? (green/yellow status) Describe or Reference SOP	Will controls be improved or implemented? (yellow or red status)			Responsible Person	Target Completion Date	
					Yes	If no, document reason.	If yes, how will this be accomplished?			
Computer Operations										
Automated jobs are scheduled and monitored by computer operations personnel through the use of an automated scheduling tool. In the event of a processing failure, the job scheduling application generates an alert. Escalation procedures and emergency call lists are available to employees to determine who to contact in the event of a processing failure, and errors are resolved and documented.	Are automated jobs scheduled and monitored by computer operations personnel through the use of an automated scheduling tool? In the event of a processing failure, does the job scheduling application generate an alert? Are escalation procedures and emergency call lists available to employees to determine who to contact in the event of a processing failure, and errors are resolved and documented?									
Full system backups are performed on a regular basis. In addition, incremental backups of critical data are performed. The agency performs an inventory audit of backups located at the offsite facility on a regular basis.	Are full system backups performed on a regular basis? In addition, are incremental backups of critical data performed regular? Does the Agency perform an inventory audit of backups located at the offsite facility on a regular basis?									
In the event that a backup job fails or data processing performance is negatively affected, a helpdesk ticket is created and computer operations personnel are responsible for investigation and documenting the resolution in the helpdesk ticket.	In the event that a backup job fails or data processing performance is negatively affected, is a notification created and are computer operations personnel responsible for investigation and documenting the resolution in the notification?									
Data Integrity										
Management establishes restrictive authorization controls within its operations including establishment of controls over source documents and data entry terminals. System analytics and exception reporting are used to ensure that all data processed are authorized.	Does management establish restrictive authorization controls within its operations including establishment of controls over source documents and data entry terminals? Are system analytics and exception reporting used to ensure that all data processed are authorized?									
Data validation procedures are in place to ensure accuracy of data manually entered and/or interfaced into the system. Data validation procedures include reconciliations to source data/system, system edit checks, and reviews of output reports.	Are data validation procedures in place to ensure accuracy of data manually entered and/or interfaced into the system? Do data validation procedures include reconciliations to source data/system, system edit checks, and reviews of output reports?									
Application controls include validation of input data, identification and resolution of rejected transactions, balancing transactions, and reconciliations (to source data, to input file, to output file).	Do application controls include validation of input data, identification and resolution of rejected transactions, balancing transactions, and reconciliations (to source data, to input file, to output file)?									
Disaster Recovery										
A disaster response and recovery plan has been developed and is understood by key personnel. As part of developing this plan, management identified and prioritized the criticality and sensitivity of computerized operations and supporting resources.	Has a disaster response and recovery plan been developed and is it understood by key personnel? As part of developing this plan, has management identified and prioritized the criticality and sensitivity of computerized operations and supporting resources?									
Management has taken steps to prevent and minimize potential damage and interruption through the use of data and program backup procedures including offsite storage of backup data as well as environmental controls, staff training, and hardware maintenance and management.	Has management taken steps to prevent and minimize potential damage and interruption through the use of data and program backup procedures including offsite storage of backup data as well as environmental controls, staff training, and hardware maintenance and management?									
Management has established a comprehensive contingency plan that allows for the timely recovery of information. This plan is periodically tested and adjusted as appropriate.	Has management established a comprehensive contingency plan that allows for the timely recovery of information? Is this plan periodically tested and adjusted as appropriate?									

Control Activities									
Best Practice Statements	Questions to Ask	    N/A	What controls are currently in place? (green/yellow status) Describe or Reference SOP	Will controls be improved or implemented? (yellow or red status)			Responsible Person	Target Completion Date	
				Yes	If no, document reason.	If yes, how will this be accomplished?			
<i>End-User Computing</i>									
Management has implemented a methodology and written policies regarding end-user computing.	Has management implemented a methodology and written policies regarding end-user computing?								
Principle Twelve: Management implements control activities through policies.									
Control activities are regularly evaluated to ensure that they are still appropriate and working as intended.	Are control activities regularly evaluated to ensure that they are still appropriate and working as intended?								
Reviews are made of actual performance compared to objectives for specific functions or activities focusing on compliance, financial, and operational issues, budgets, and performance in prior periods for all major initiatives. Management analyzes and follows up as needed.	Are reviews made of actual performance compared to objectives for specific functions or activities focusing on compliance, financial, and operational issues, budgets, and performance in prior periods for all major initiatives. Does management analyze and follow up as needed?								
Management documents in policies the internal control responsibilities of the agency which could include the day-to-day procedures and timing of certain control activities within the agency. Management communicates to personnel the policies and procedures so that personnel can implement the control activities for their assigned responsibilities.	Does management document in policies the internal control responsibilities of the agency which could include the day-to-day procedures and timing of certain control activities within the Agency/AU? How does management communicate to personnel the policies and procedures so that personnel can implement the control activities for their assigned responsibilities?								

Information and Communication Internal Control Evaluation (ICE) Template

(an optional tool to be used in conjunction with the Uniform Compliance Guidelines on Internal Controls for State and Quasi Agencies)

Agency _____

Evaluator: _____

Date of Evaluation: _____

Information and Communication											
					Will controls be improved or implemented? (yellow or red status)						
Best Practice Statements	Questions to Ask					What controls are currently in place? (green/yellow status)	Yes	If no, document reason.	If yes, how will this be accomplished?	Responsible Person	Target Completion Date
Principle Thirteen: Management uses quality information to achieve agency objectives.											
Management continuously identifies its information requirements needed to communicate effectively both internally and externally. This would include management's review of changes to statute, regulations, economic changes, and other factors.	How does management continuously identify changes (e.g., control environment, internal controls, regulations) and ensure changes are communicated internally and/or externally?										
Management obtains relevant data from reliable internal and external sources in a timely manner based on the identified information requirements.	Where and when does management obtain its relevant data (both internally and externally) and how does management ensure that information received is reliable and not false information?										
Management processes the obtained data into quality information that supports the internal control system and is effectively communicated throughout the agency's information system.	Is management using current, complete, accurate, and accessible information on a timely basis to make informed decisions? What reporting mechanisms are being used to run reports to meet the control objectives?										
Principle Fourteen: Management internally communicates the necessary quality information to achieve agency objectives.											
Policies and procedures are formally shared with employees, up-to-date, reflective of actual operating practices, in alignment with goals and objectives, and comply with state and federal program requirements.	How are changes (e.g., policy/procedural, compliance, or regulatory) communicated to employees? Are policies and procedures reviewed and updated to reflect changes?										
Management ensures that effective <u>internal</u> communications occur (e.g. risk management, employee specific duties, acceptable/unacceptable behavior, complaints/inquiries, system to have improvements recommended or operations, employee recognition).	How does management ensure that effective internal communications occur (e.g. risk management, employee specific duties, acceptable/unacceptable behavior, complaints/inquiries, employee recognition)? Is there a system to receive and evaluate recommendations for improvement?										
Management promotes and fosters trust between employees, supervisors and other parties by establishing open channels of communication.	Are there open channels of communication in the agency? What is the policy for staff to be able to communicate with management, including any deficiencies in controls that staff may notice?										

Information and Communication

					Will controls be improved or implemented? (yellow or red status)							
					Yes	If no, document reason.	If yes, how will this be accomplished?	Responsible Person	Target Completion Date			
Best Practice Statements	Questions to Ask	★	▲	●	N/A	What controls are currently in place? (green/yellow status)						
An effective whistleblower protection program and fraud hotline is in place and its existence and procedures are known to all employees.	Does an effective whistleblower protection program and fraud hotline exist? Where can this information be found? How is this information communicated to employees?											
Management periodically evaluates the accuracy, timeliness and relevance of its information and communication systems. Management questions information on management reports that appears unusual or inconsistent.	What is the process and timeframe to review reports received from staff to evaluate accuracy, timeliness, and relevance of information?											
Principle Fifteen: Management externally communicates the necessary quality information to achieve agency objectives.												
Management ensures that effective external communications (e.g. open channels with customers, suppliers, contractors, consultants, other governments; complaints/inquiries, advice from outside parties) occur with groups that can have a serious impact on programs, projects, operations, and other activities, including budgeting and financing.	Does management have effective communications with external parties? If yes, how does management promote these effective communications (e.g., presentations, annual reports, press releases, newsletters)?											
An effective whistleblower protection program and fraud hotline is in place and its existence and procedures are known to all vendors, contractors, and business partners.	Does an effective whistleblower protection program and fraud hotline exist? Where can this information be found? How is this information communicated to all vendors, contractors, and business partners?											
Appropriate management reviews occur prior to report submission to parties outside the agency.	Does management use professional judgement regarding what information needs to be reviewed before being released to external parties? If yes, is this documented in a policy or procedure?											

Monitoring Internal Control Evaluation (ICE) Template

(an optional tool to be used in conjunction with the Uniform Compliance Guidelines on Internal Controls for State and Quasi Agencies)

Agency: _____

Evaluator: _____

Date of Evaluation: _____

Monitoring						Will controls be improved or implemented? (yellow or red status)						
Best Practice Statements	Questions to Ask						What controls are currently in place?(green/yellow status). Describe or Reference SOP	Yes	If no, document reason.	If yes, how will this be accomplished?	Responsible Person	Target Completion Date
Principle Sixteen: Management establishes and operates monitoring activities to monitor the internal control system and evaluate the results.												
Management establishes a baseline to monitor the internal control system.	Has management established a baseline to monitor the internal control system?											
Management monitors the internal control system through ongoing monitoring and separate evaluations. Ongoing monitoring includes regular management and supervisory activities, comparisons, reconciliations, and other routine actions. Separate evaluations include self-assessments as well as audits and other evaluations performed by internal auditors, external auditors, and other external reviewers. Monitoring of the internal control system includes evaluations of the internal controls at the subrecipient and vendor level, when applicable.	How does management monitor the internal control system on an ongoing basis? Does management perform separate evaluations in addition to ongoing monitoring? Does management perform these tasks for all appropriate personnel, including the subrecipient and vendor level when applicable?											
Management undergoes a systematic review and evaluation of each critical business process.	Does management periodically complete a review and evaluation of each mission critical process?											
Management provides oversight on securing audit reports of its service organizations and directs them to all pertinent parties for review and follow-up of deficiencies identified in the reports (if applicable).	Does management obtain the appropriate reports (e.g., SOC reports) from all outside third-party vendors and follow up on deficiencies noted in the reports. If yes, how does management follow up on these deficiencies?											
Management evaluates and documents the results of ongoing monitoring and separate evaluations to identify internal control issues and uses this evaluation to determine the effectiveness of the internal control system.	How does management document the results of its ongoing monitoring and separate evaluations of internal controls?											
Management identifies changes in the internal control system that either have occurred or are needed because of changes in the agency.	How does management assess whether significant changes need to be addressed in the internal control system?											
Principle Seventeen: Management remediates identified internal control deficiencies on a timely basis.												
Mechanisms are in place for employees to report deficiencies in internal control to management on a timely basis.	How do employees report deficiencies in internal control to management?											
Management evaluates and documents internal control issues, both identified internally or via external review/audit, and determines appropriate corrective action for internal control deficiencies on a timely basis.	How does management evaluate and document internal control issues, both identified internally or via external review/audit, to determine appropriate corrective action on a timely basis? Is management responsive to findings and recommendations of audits and other reviews? Are corrective actions monitored?											

Tools for Development Overview with Links

(Optional evaluation tools to be used in conjunction with Uniform Compliance Guidelines on Internal Controls for State and Quasi Agencies)

Tools and examples provided in this section may be used in conjunction with steps in the Uniform Compliance Guidelines on Internal Controls for State and Quasi Agencies. Management may modify these tools or use other methods as deemed appropriate to evaluate, develop, and document the internal control system.

Control Environment

After evaluation, management may determine that improvements should be made to the control environment. The following optional tools follow steps provided in Part Two, Section One, "*Developing the Control Environment*." However, management may choose any method that best suits the needs of the agency. If using the tools provided, management will want to **choose one** of the following –

Control Environment Questionnaire. This document walks through the steps in "*Developing the Control Environment*" with examples of activities to improve the control environment and space to document controls or references to agency policies. The questionnaire may be downloaded for agency use at this link. [\[Outside Link\]](#)

Control Environment Development Template. This spreadsheet provides an abbreviated method for management to design control environment processes by following the steps in "*Developing the Control Environment*" and document controls or references to agency policies. The template may be downloaded for agency use at this link. [\[Outside Link\]](#)

In conjunction with either tool, management may refer to *Example Objectives, Risks, and Controls* for ideas on objectives and risks related to the control environment. [\[Link\]](#)

Conducting a Risk Assessment

Risk assessment involves an ongoing process to recognize potential problems (risks) and determine the best way to manage them. When considering ways to conduct a risk assessment, management may wish to consider the following tool, which follows the steps outlined in Part Two, Section Two, "*Conducting a Risk Assessment*."

Risk Assessment Template. The Risk Assessment Template provides a method for management to document risks to objectives and management's response to those risks. This template follows the outlined steps in "*Conducting a Risk Assessment*." The template may be downloaded for agency use at this link. [\[Outside Link\]](#)

In conjunction with this tool, management may refer to *Example Objectives, Risks, and Controls* for ideas on objectives and risks for major transaction areas. [\[Link\]](#)

Tools for Development Overview

(Continued)

Control Activities, Information and Communication, and Monitoring

After conducting a risk assessment, management develops processes to mitigate identified risks by implementing control activities, information and communication, and monitoring processes. Management may **choose one** available tool or other method suitable for the agency's needs.

Control Development Template. This spreadsheet provides an abbreviated method for management to design and document control activities, information and communication, and monitoring processes to address specific risks identified through the risk assessment process. This template follows steps outlined in the *Uniform Compliance Guidelines on Internal Controls for State and Quasi Agencies* for developing control activities, information and communication processes, and monitoring procedures. Several risks may be addressed on this template. The template may be downloaded for agency use at this link. [\[Outside Link\]](#)

Control Development Questionnaire. This questionnaire walks through the steps outlined in the *Uniform Compliance Guidelines on Internal Controls for State and Quasi Agencies* for developing control activities, information and communication processes, and monitoring procedures. Space is provided to explain and document internal controls to mitigate the identified risk. The questionnaire may be downloaded for agency use at this link. [\[Outside Link\]](#)

In conjunction with either tool, management may refer to *Example Objectives, Risks, and Controls* for ideas on objectives, risks, and controls for major transaction areas. [\[Link\]](#)

Examples Overview

Internal controls must be continually evaluated and developed to meet agency needs. The following examples are intended to generate ideas for the design of an internal control system and illustrate the use of certain tools provided. Because state and quasi agencies vary in size and complexity, no single method or set of internal control policies and procedure universally applies.

Objectives, Risks, and Controls

This document provides examples of objectives, risks, and key controls for the control environment and major transaction areas. Lists are not intended to be exhaustive or applicable to all agencies. The control environment and major transaction areas contain some or all the following examples categories:

- Example Objectives and Risks
- Minimum Internal Control Standards per the Accounting and Uniform Compliance Guidelines Manual for State and Quasi Agencies
- Example Key Controls

Examples include the following areas:

- Control Environment
- Financial Reporting
- Budget Reporting
- Cash Receipts
- Accounts Receivable
- Purchasing / Accounts Payable
- Human Resources
- Inventory
- Capital Assets
- Information Technology

Risk Assessment Template – [Example Tab](#)

This risk assessment template displays an example entry for one aspect of safeguarding cash collections. The template is for illustration purposes only; it is not a complete analysis of all risks to the cash collection process.

Control Development Template – [Example Tab](#)

This control development template shows example entries for controls related to the cash receipts process. This is not intended to be a complete list of controls. The example template is for illustration purposes only; it is not a complete analysis of all risks and controls for the cash collection process.

Control Environment

Example Objectives and Risks

Example Objectives	Example Risks
<p>Management recognizes the importance of and commitment to the establishment and maintenance of a strong system of internal control as communicated to all employees through actions and words.</p> <p>Management adheres to a code of conduct and other policies regarding acceptable business practices, conflicts of interest, or expected standards of ethical and moral behavior, and communicates these policies to all employees.</p>	<ul style="list-style-type: none"> • Employees lack knowledge of internal controls. • Code of conduct and/or ethics policy has been inadequately communicated (i.e., intranet, posters, memorandum, etc.) or does not exist.
<p>Organizational structure units are clearly defined and up to date to perform the necessary functions and determine that appropriate reporting relationships have been established.</p>	<ul style="list-style-type: none"> • Organizational chart is not current. • Employees unaware of reporting relationship in the organizational structure. • Duplication of functions by units.
<p>Personnel are qualified and properly trained for the functions in order for control procedures to operate in the manner intended.</p> <p>Current job descriptions are established detailing the responsibilities and qualifications for each position.</p>	<ul style="list-style-type: none"> • Personnel not qualified to perform tasks assigned. • Personnel not adequately trained. • Lack of continuing education for personnel. • Job descriptions not coordinated with actual job performances.

Control Environment

Example Objectives and Risks (Continued)

Example Objectives	Example Risks
Delegation of authority or limitation of authority exists to provide assurances that responsibilities are effectively discharged.	<ul style="list-style-type: none"> • One employee controls all phases of a transaction. • Management goals are not communicated to staff employees.
Policies and procedures are documented and provide a basis for reviews, follow-up evaluations and audits.	<ul style="list-style-type: none"> • Functions are not performed uniformly. • Statutory requirements not being met. • Lack of support for functions and transactions performed.
Budgetary and reporting practices provide benchmarks by which management can measure accomplishments.	<ul style="list-style-type: none"> • Management does not have guidelines to measure performance. • Management cannot communicate expectations to the departments. • Unusual transactions or events cannot be detected. • Management cannot determine if goals are being achieved.
Organizational checks and balances provide authority for certain functions that minimize the potential for waste, fraud, abuse, or mismanagement.	<ul style="list-style-type: none"> • Departments do not perform responsibilities; therefore, the potential for waste, fraud and abuse can occur.

Financial Reporting

Example Objectives and Risks

Example Objectives	Example Risks
All transactions are properly accumulated, classified, and summarized in the accounts.	<ul style="list-style-type: none"> • General ledger not in balance. • Subsidiary ledgers not in balance with general ledger. • Inconsistent application of accounting policies and procedures.
All closing entries are initiated by authorized personnel and reviewed and approved in accordance with established policies and procedures.	<ul style="list-style-type: none"> • Inadequate closing procedures may result in confusion of responsibility, delay in completing the closing. • Transactions improperly included or excluded as a result of inadequate cutoff procedures. • Unauthorized or inappropriate journal entries. • Inadequate support for journal entries.
All necessary data is obtained and processed in accordance with established policies and procedures.	<ul style="list-style-type: none"> • Absence of adequate procedures may result in misclassification of balances, omission of an accounting unit, unacceptable delays, and excessive work. • Omission of information which should be provided in financial reports, lack of control over data submitted and review process.
All internal and public financial reports are prepared on the basis of appropriate supporting data, provide required information, and are reviewed and approved before issuance.	<ul style="list-style-type: none"> • Financial reports not supported by underlying accounting records. • Inconsistent presentation of financial data. • Incomplete review of data, permitting possible errors or omissions.

Financial Reporting

Example Key Controls

Reconciliations of subsidiary ledgers to control accounts are prepared and reviewed by someone other than the preparer.

Journal entries are prepared and reviewed by someone other than the preparer.

Financial statements and note disclosures agree to underlying supporting documentation.

Financial statement information and note disclosures are reviewed and approved by knowledgeable staff.

Management identifies accounts, such as accounts involving complex calculations or accounting estimates that are especially at risk of misstatement and develops policies and procedures to address those risks timely.

Budget Reporting

Example Objectives and Risks

Example Objectives	Example Risks
Preparation of a budget, whether or not legally required, which internally and externally communicates goals and objectives and serves as a "benchmark" against which actual performance is measured.	<ul style="list-style-type: none"> • No practical means by which to measure performance. • Internal departments and staff unsure of goals of the executive. • Absence of effective control over expenditures.
Obtain assurance that expenditures are incurred in conformity with the budget and plan of operations.	<ul style="list-style-type: none"> • Violation of law. • Expenditures incurred in excess of budget authorization. • Arbitrary or unauthorized transfers between budget categories.
Budget versus actual reporting is provided on a timely basis and explanations are provided for significant deviations.	<ul style="list-style-type: none"> • Lack of timely information on budget versus actual status prohibits corrective action. • Department managers unaware of status of their budget and potentially prohibited from executing plans. • Unbudgeted actual transactions may not be detected.

Budget Reporting

Example Key Controls

Actual expenditures and revenues are compared to budgeted amounts monthly and on a timely basis.

Budget revisions are approved by an authorized person before being entered into the accounting system.

Expenditures or under-realized revenues are discussed with departmental personnel; significant variations from budgeted amounts are explained.

Cash Receipts

Example Objectives and Risks

Example Objectives	Example Risks
All collections are properly identified, control totals developed, and collections promptly deposited intact.	<ul style="list-style-type: none"> • Failure to record cash receipts. • Withholding or delaying the recording of cash receipts. • Incorrect recording in the accounting system.
All bank accounts and cash on hand are subject to effective custodial accountability procedures and physical safeguards.	<ul style="list-style-type: none"> • Misappropriated cash or petty cash funds; diverted cash receipts; unauthorized cash disbursements; loss of funds.
All transactions are promptly and accurately recorded in adequate detail and appropriate reports are issued.	<ul style="list-style-type: none"> • Concealing unauthorized transactions or misappropriated collections by substituting unsupported credits or fictitious expenditures. • Under or overestimating cash or receivables.
All transactions are properly accumulated, correctly classified, and summarized in the general ledger; balances are properly and timely reconciled with bank statement balances.	<ul style="list-style-type: none"> • Misstating cash balances • Concealing unauthorized transactions by falsifying bank reconciliations.

Cash Receipts

Minimum Internal Controls per the Accounting and Uniform Compliance Guidelines Manual for State and Quasi Agencies Chapter 4 – Accounting for Revenue

Mail possibly containing checks, money orders, or cash should be opened by two people.

Money received should be recorded at time of receipt.

Checks should also be restrictively endorsed, and date stamped upon receipt. This should occur upon opening the mail or otherwise receiving the instrument (check).

A complete listing of collections received should be made by a person independent of the duties of processing the receipts or making deposits. Editing of the listing should be restricted to initial recorder and the reconciler.

All receipts, licenses, or other accountable items must be pre-numbered or sequentially numbered by computer when issued.

Documents should be used in sequential order. If the volume warrants, a separate numeric series should be used for different revenue sources.

Licenses, permits, goods for sale, invoices, etc., are considered accountable items for which a corresponding deposit must be made.

Receipts should be issued and recorded at the time of the transaction; for example, when cash or a check is received, a receipt is to be immediately prepared and given to the person making payment.

Licenses, permits, and other accountable items should be issued timely.

Collections must be deposited intact. Deposits are to be made within the next business day in compliance with IC 5-13-6-1.

Safeguard the collections through locked drawers, cabinets, or safes, particularly during breaks, lunchtime, and overnight.

Cash, receipts, books, licenses, etc., should be inaccessible to unauthorized persons.

Collections and other accountable items should reconcile to the bank statements and the agency's cash book. There is no authority for an agency to maintain an "over" or "short" fund.

The duties of collecting monies, processing the receipt, license, permit, etc., preparing and making deposits, and performing reconciliations should be segregated to the fullest extent possible considering the size of the agency and the materiality of collections.

Supporting documentation for monies received must be maintained and made available for audit to provide supporting information for the validity and accountability of monies received.

Documents must be filed in such a manner as to be readily accessible, or otherwise reasonably attainable, upon request during an audit.

Cash Receipts

Example Key Controls

Duties are segregated so that the following responsibilities performed by different people:

- Custody of the funds, reconciliation of the funds and access to cash receipts.
- Completing the disbursement receipts, disbursement, and reconciliation.
- Making a deposit, billing, making General Ledger entries and collecting.
- Collecting cash, balancing cash, closing cash registers, making a deposit, maintaining Accounts Receivable records, and making General Ledger entries.
- Collecting of licenses, fines, and inspections (etc.) and making General Ledger entries.
- Collecting cash and reconciling the bank account.
- Reconciling Cash registers daily by a person not involved in cash receipting.
- Preparing the deposit and verifying the validated bank deposit slip.
- Preparing and approving bank account reconciliations and investigation of unusual reconciling items are segregated from other cash receipts or disbursement functions.
- Cash receipts are reconciled (cash, checks, credit cards, wires) on a daily basis to the total dollar value sold. (For example, total dollar amount reconciled to number of licenses issued.)
- Management reviews and approves bank reconciliations on a monthly basis.
- Timely corrective actions are taken in cash discrepancies.

Accounts Receivable

Example Objectives and Risks

Example Objectives	Example Risks
<p>Ensure that appropriate records are maintained for all businesses, users of government services, and individuals or entities against who taxes or fees are assessed.</p>	<ul style="list-style-type: none"> • Government loss of revenue as a result of billing errors. • Eligible parties who have failed to file tax or other informational returns not identified. • Systems may permit unauthorized removal of taxpayers or others from rolls. • Employees' diversion of revenue for personal use.
<p>Billing of taxes and services is performed promptly and in proper amounts; self-assessed taxpayers monitored; exemptions are only provided to those authorized.</p>	<ul style="list-style-type: none"> • Billings inaccurately or incompletely prepared resulting in excess/loss of revenue and inaccurate accounting. • Sales, income, and other self-assessed taxpayers may pay amounts less than required by law. • Revenue lost due to inadequate procedures or improper accounts. • Policies and procedures insufficient to collect amounts in a timely manner.
<p>All collections are properly identified, control totals developed, and collections promptly deposited intact and applied to the proper accounts.</p>	<ul style="list-style-type: none"> • Withholding or delaying the recording of cash receipts and application of funds to the proper accounts. • Employee diversion of receipts for personal use. • Failure to receive proper distribution of taxes collected by another level of government. • Amounts improperly written-off and collections diverted to personal use.

Accounts Receivable

Example Objectives and Risks (Continued)

Example Objectives	Example Risks
<p>Billings, adjustments, and collections are properly recorded in individual receivable accounts.</p>	<ul style="list-style-type: none"> • Account balances reduced by unauthorized transactions. • Cash flow from payments delayed by late billings or deposits.
<p>Revenues, collections, and receivables are properly accumulated, classified, and summarized in the accounts.</p>	<ul style="list-style-type: none"> • Errors in transaction postings to detail or control accounts not detected in a timely manner. • Problem accounts do not receive prompt attention, resulting in revenue or cash-flow loss. • Improper revenue receivables accounting policies and practices result in misstatement of account balances.

Accounts Receivable

Minimum Internal Controls per the Accounting and Uniform Compliance Guidelines Manual for State and Quasi Agencies Chapter 4 – Accounting for Revenue

Mail possibly containing checks, money orders, or cash should be opened by two people.

Money received should be recorded at time of receipt.

Checks should also be restrictively endorsed, and date stamped upon receipt. This should occur upon opening the mail or otherwise receiving the instrument (check).

A complete listing of collections received should be made by a person independent of the duties of processing the receipts or making deposits. Editing of the listing should be restricted to initial recorder and the reconciler.

All receipts, licenses, or other accountable items must be pre-numbered or sequentially numbered by computer when issued.

Documents should be used in sequential order. If the volume warrants, a separate numeric series should be used for different revenue sources.

Licenses, permits, goods for sale, invoices, etc., are considered accountable items for which a corresponding deposit must be made.

Receipts should be issued and recorded at the time of the transaction; for example, when cash or a check is received, a receipt is to be immediately prepared and given to the person making payment.

Licenses, permits, and other accountable items should be issued timely.

Collections must be deposited intact. Deposits are to be made within the next business day in compliance with IC 5-13-6-1.

Safeguard the collections through locked drawers, cabinets, or safes, particularly during breaks, lunchtime, and overnight.

Cash, receipts, books, licenses, etc., should be inaccessible to unauthorized persons.

Collections and other accountable items should reconcile to the bank statements and the agency's cash book. There is no authority for an agency to maintain an "over" or "short" fund.

Collections and other accountable items should reconcile to the bank statements and the agency's cash book. There is no authority for an agency to maintain an "over" or "short" fund.

The duties of collecting monies, processing the receipt, license, permit, etc., preparing and making deposits, and performing reconciliations should be segregated to the fullest extent possible considering the size of the agency and the materiality of collections.

Supporting documentation for monies received must be maintained and made available for audit to provide supporting information for the validity and accountability of monies received.

Documents must be filed in such a manner as to be readily accessible, or otherwise reasonably attainable, upon request during an audit.

Accounts Receivable

Example Key Controls

Duties are segregated so that the following responsibilities performed by different people:

- Custody of the funds, reconciliation of the funds and access to cash receipts.
- Completing the disbursement receipts, disbursement, and reconciliation.
- Making a deposit, billing, making General Ledger entries and collecting.
- Collecting cash, balancing cash, closing cash registers, making a deposit, maintaining Accounts Receivable records, and making General Ledger entries.
- Collecting of licenses, fines, and inspections (etc.) and making General Ledger entries.
- Collecting cash and reconciling the bank account.
- Reconciling Cash registers daily by a person not involved in cash receipting.
- Preparing the deposit and verifying the validated bank deposit slip.
- Responsibilities for preparing and approving bank account reconciliations and investigation of unusual reconciling items are segregated from those for other cash receipts or disbursement functions.
- Total cash receipts (cash, checks, credit cards, wires) are reconciled on a daily basis to the total dollar value sold. (For example, total dollar amount reconciled to number of licenses issued.)
- Does management review and approve bank reconciliations on a monthly basis.
- Are timely corrective actions taken in cash discrepancies.
- Write-offs or adjustments have proper authorizations.
- Subsidiary accounts receivable and notes receivable records are maintained and reconciled monthly with the general ledger control account.
- Duties are segregated so that the following responsibilities performed by different people:
- Billing and collecting of accounts receivable funds.
- Maintenance of detail accounts receivable records, collections, and general ledger posting.

Accounts Receivable

Example Key Controls (Continued)

- Writing off or adjusting to accounts receivable and maintenance of accounts receivable records.
- Investigating disputes with billing amounts and maintenance of accounts receivable records.
- Reconciling, investigating reconciling items, and posting detail accounts receivable records.
- Is access to the accounts receivable accounting system limited only to authorized individuals.
- Corrections and adjustments to cash receipts are documented and approved by management.
- Non-cash credits, such as credit memos, allowances, and bad debts are properly authorized.
- An aging schedule is prepared monthly and reviewed by management.
- Accounts are reviewed by someone independent of cash and accounts receivable accounting.

Purchasing / Accounts Payable

Example Objectives and Risks

Example Objectives	Example Risks
All requests for goods and services are initiated and approved by authorized individuals and are in accordance with budget and appropriation guidelines.	<ul style="list-style-type: none"> • Purchases from unauthorized vendors. • Purchases are in violation of a conflict-of-interest policy. • Purchases are not timely. • Purchases not in accordance with budget and/or appropriations provisions.
All purchase orders are based on valid, approved requests and are properly executed as to price, quantity, and vendor.	<ul style="list-style-type: none"> • Payment in excess of optimum price. • Quantities not adequate or in excess of need.
All materials and services received agree with the original orders.	<ul style="list-style-type: none"> • Payment for materials or services not received. • Damaged or missing goods not reported.
All invoices processed for payment represent goods and services received and are accurate as to terms, quantities, prices, and extensions; account distributions are accurate and agree with established account classifications.	<ul style="list-style-type: none"> • Payment based on improper price or terms. • Accounting distribution of cost is inaccurate.
All checks are prepared on the basis of adequate and approved documentation, compared with supporting data, and are properly approved, signed and mailed.	<ul style="list-style-type: none"> • Incorrect or duplicate payments. • Alteration of checks. • Disbursement for materials or services not properly documented or approved.
All disbursement, accounts payable, and encumbrance transactions are promptly and accurately recorded as to payee and amount.	<ul style="list-style-type: none"> • Improper cash, accounts payable and encumbrance balances.
All entries to accounts payable, reserve for encumbrances, asset and expense accounts, and cash disbursements are properly accumulated, classified, and summarized in the accounts.	<ul style="list-style-type: none"> • Misstated financial statements. • Misstated internal financial data.

Purchasing / Accounts Payable

Minimum Internal Controls per the Accounting and Uniform Compliance Guidelines Manual for State and Quasi Agencies Chapter 5 - Procurement

If one individual is responsible for the requisition, purchasing, and receiving functions, fictitious or unauthorized purchases can be made. This may result in the theft of goods and possibly payment for unauthorized purchases.

Roles approved by the Financial Policy Group and set up by GMIS are designed to reduce the risk of collusion and unauthorized purchasing to a relatively low level. It is recommended that the various roles be assigned to separate individuals. The basic underlying rule is "no one should be able to approve his/her own work." Also, no one can obtain a 'working' role without completing the applicable training.

General rules for approval roles are:

- It is highly recommended that an Approver complete the training for related modules.
- An Approver should not approve his/her own work.
- An Approver should be at a higher level of authority than the originator; if this is not possible, should be at the same level, but in a different department.
- An Approver should never be at a lower level of authority than the originator.
- An Approver should be knowledgeable about the process/purchase in order to authorize.
- An Approver is ultimately responsible for all entries in the transaction, including chart fields and accounting entries.

An employee who has been designated as Procurement Agent/Buyer for an agency after satisfactorily completing applicable IDOA courses may be assigned to Requisition, RFP, and PO roles if the following conditions are met:

- Requisitioner records Requestor (if different) and requisition is approved by 1) ProcAgent and; 2) FISCAL (see role names below).
- PO is then to be approved by the agency Head Procurement Agent or IDOA (if applicable).

Purchasing / Accounts Payable

Minimum Internal Controls per the Accounting and Uniform Compliance Guidelines Manual for State and Quasi Agencies Chapter 5 - Procurement (Continued)

The following are definitions of ePro entry and approval roles:

- SOI_Ag_Proc_Agent – Procurement Agent – Delegated by IDOA; if more than one, a Head Procurement Agent is determined.
- SOI_Ag_Fiscal – Fiscal approver – Usually CFO or director of accounting department – must have knowledge of accounting rules, chart of accounts, etc.

NO ONE should hold both of the above roles. Agency designated "SOI_ePro_Buyer" can hold the SOI_Ag_Proc_Agent role.

Additional levels may be added, as requested by the agency, for certain types or cost of purchases.

The ePro system will automatically route requisitions through the approval system as required for each type of purchase. Approvals may be required of the Commission on Public Records (ICPR), the Office of Technology (IOT), or the Department of Administration (IDOA) Procurement Division, Motor Pool, Budget Agency, PEN Products and/or IN-ARF. Necessary budget checks will be processed automatically prior to agency supervisory approvals.

Purchasing / Accounts Payable

Minimum Internal Controls per the Accounting and Uniform Compliance Guidelines Manual for State and Quasi Agencies Chapter 6 – Expenses / Expenditures

Separation of duties is critical to internal control for processing payables and expenses (or expenditures).

Care must be taken to assure that all invoices are recorded timely and accurately and that all purchases are authorized. PeopleSoft Financials roles designed to provide this assurance are discussed in Chapter 2, Internal Controls.

Those with workflow approvals are responsible for certifying the accuracy of all information on the document they are approving.

The person verifying the count of product and entering the receiver into the system should be independent of both the purchasing and invoicing functions. Exceptions to this rule are granted by the internal control group in certain situations where the actual receiver of the product does not have system access; in these cases, the actual receiver must sign and date the bill of lading and then pass it on to the AP Receiver, who is responsible for retaining these documents for audit purposes.

All purchase orders and receiving reports should be matched to invoices, with follow-up on inconsistent information.

Individuals independent of the purchasing and receiving functions should follow up on mismatched or unmatched, missing, or duplicate items.

Vendor statements should be reconciled to accounts payable items.

Returns and allowances credit memos should be matched to shipping orders and/or vendor communications.

Individuals independent of the accounts payable function should follow up on unmatched shipping orders for returned goods and related receiving reports and invoices and resolve missing, duplicate, or unmatched items.

Any subsidiary ledgers should be reconciled with purchase and cash disbursement transactions, and differences resolved.

Access to accounts payable and related files should be restricted.

Warrants and remittance advices should be verified and mailed without allowing them to return to the staff that prepared claims or approved the transactions for payment.

Warrants should be verified in a timely manner and retained in a secure location until mailed.

Purchasing / Accounts Payable

Minimum Internal Controls per the Accounting and Uniform
Compliance Guidelines Manual for State and Quasi Agencies
Chapter 6 – Expenses / Expenditures
(Continued)

An approver role should not be taken lightly, as this is a very important segment of the internal control process. A few basic rules apply when assigning these roles:

- An approver should be at a higher level of authority than the originator of the transaction; exceptions might be made if the approver is 1) in another department and 2) has a working knowledge of the accounting and recording of the transaction. However, the approver should never be at a lower level of authority.
- An approver is responsible for authorizing the payment and for certifying the accuracy of all information on the transaction, including, but not necessarily limited to:
 - o Chart field values
 - o Dollar amount
 - o Vendor information, including remit to address

An approver should confirm that PO vouchers are copied from PO receipts.

Purchasing / Accounts Payable

Minimum Internal Controls per the Accounting and Uniform
Compliance Guidelines Manual for State and Quasi Agencies
Chapter 10 – Travel

Each state agency should establish controls to ensure that all payments and reimbursements for travel expenses are legitimate, accurate and in compliance with State travel rules and regulations. Travel reimbursements should not be made for travel of a personal nature.

All claims for reimbursement should be approved by an authorized person.

Purchasing / Accounts Payable

Example Key Controls

Purchase orders or contracts are approved by appropriately designated persons before issuance.

Changes to contracts or purchase orders are subject to the same controls and approvals as the original agreement.

Duties are segregated so that the following responsibilities performed by different people:

- Requisitioning, purchasing, and receiving functions and the invoice processing, accounts payable, and general ledger functions.
- Purchasing, requisitioning, and receiving.
- Invoice processing and making entries to the general ledger.
- Preparation of cash disbursements, approval, and entries to the general ledger.
- Making detail cash disbursement entries and entries to the general ledger.

Disbursements are approved for payment only by properly designated persons.

The individual responsible for approval is furnished with invoices and supporting data to be reviewed prior to approval.

Adjustments of recorded accounts payable or other liabilities are properly approved.

Requests for progress payments under long-term contracts are formally approved by a designated contract administrator with formal approval authority.

P-card purchases are reconciled monthly by someone other than the cardholder.

Human Resources

Example Objectives and Risks

Example Objectives	Example Risks
Additions, separations, wage rates, salaries, and deductions are authorized and documented. Payroll and personnel policies are in compliance with grant agreements and federal and state laws.	<ul style="list-style-type: none"> • Unauthorized or fictitious names are added to the payroll. • Payments continued to terminated employees. • Wage rates and salaries used are at a higher rate than authorized. • Payroll reimbursement through grant funding denied. • Penalty for noncompliance with federal and state laws.
Employees' time and attendance data are properly reviewed and approved.	<ul style="list-style-type: none"> • Employees are paid for time which they did not work. • Employees are paid for time which was unnecessary or unauthorized.
Employees' time and attendance data are properly processed and documented and accurately coded for account distribution.	<ul style="list-style-type: none"> • Employees are paid for time which they were absent from work. • Errors in coding of accounting distribution for payroll costs.
Computations for gross pay, deductions, and net pay are accurate and based on authorized time and rates; the recording and summarization of payments to be made and cost to be distributed are accurate and agree with established account classifications.	<ul style="list-style-type: none"> • Employee compensation and payroll deductions are computed erroneously. • Payroll and related costs are not distributed in accordance with established account classification. • Reimbursable payroll costs are not recovered under grant or shared cost programs. • Amounts paid at rates different than those authorized.

Human Resources

Example Objectives and Risks (Continued)

Example Objectives	Example Risks
Payments for employee compensation and benefits are made to or on behalf of only bona fide employees for services performed as authorized.	<ul style="list-style-type: none">• Payments made to unauthorized individuals.• Employees paid for unauthorized benefits.
Employee compensation and benefit costs are properly accumulated, classified, and summarized in the accounts.	<ul style="list-style-type: none">• The accounting distribution of payroll and related costs are classified improperly.• Accrued liabilities or disclosures for employee benefits are misstated.

Human Resources

Minimum Internal Controls per the Accounting and Uniform Compliance Guidelines Manual for State and Quasi Agencies Chapter 9 – Payroll and Personnel Transactions

Regardless of the system used in time collection and to process payroll transactions, an internal control system should be in place to assure correctness and accuracy on payroll related documents.

T&L electronic submissions must be approved by a supervisor.

The approval should be by a direct supervisor who has knowledge of the employee's attendance.

The electronic submissions and approvals are considered adequate documentation of the control activities; it is not required to print the attendance report.

If an agency is not yet utilizing Time and Labor, attendance reports should be dated as of the last day worked, should be signed by the employee, and should be approved by a direct supervisor who has knowledge of the employee's attendance.

Human Resources

Example Key Controls

Approved notices of additions, separations, and changes in salaries, wages, and deductions are reported according to the payroll scheduled cut-off date.

Terminated employees are interviewed as a physical check on departures and as a final review of the termination settlement to ensure that all keys, equipment, credit cards, etc., are returned.

Completed payroll transmittals are reviewed and approved by a responsible official before processing.

Payroll registers are reconciled to the payroll accounts in the general ledger by a knowledgeable person not otherwise involved in payroll processing.

Individual employee time and attendance records are:

- Prepared and signed by each employee for each pay period.
- Sufficiently detailed to show time charged properly.
- Reviewed and signed by each employee's supervisor.
- Reconciled with centralized time and attendance records.

Hours worked, overtime hours, compensatory time, and other special benefits (on-call, shift premium) are reviewed and approved by the employee's supervisor.

Individual employee leave records are reconciled, at least annually, to appropriate records maintained for accumulated employee benefits (vacation, sick leave, etc.).

Inventory

Example Objectives and Risks

Example Objectives	Example Risks
All transactions are approved by authorized individuals.	<ul style="list-style-type: none"> • Purchase of unauthorized materials acquired in excess of need, at appropriate prices, or at unfavorable terms.
All inventory items are subject to effective custodial accountability procedures and physical safeguards.	<ul style="list-style-type: none"> • Theft by employees or outsiders; inadequate insurance coverage.
All receipts and withdrawals of inventory are properly recorded, and the records reflect actual quantities on hand.	<ul style="list-style-type: none"> • No basis for comparing actual usage with expected usage; inability to determine material reorder points.
All transactions are properly accumulated, classified, and summarized in the accounts.	<ul style="list-style-type: none"> • Misstated financial statements; concealment of shortages.

Inventory

Example Key Controls

The agency maintains perpetual inventory records, and inventory items are put in the perpetual inventory system.

Receiving reports are used to record purchases to the perpetual inventory records.

Duties are segregated so that the following responsibilities performed by different people:

- Receiving and issuing of inventory and the operational duties.
- Receiving and issuing of inventory and taking the physical inventory.
- Receiving and issuing of inventory and approving expenditures, recording transactions in the general ledger, and reconciliation of subsidiary records to control accounts.

Work orders or requisitions are required to be approved by appropriately designated persons as a basis of issuing inventories.

Physical access to inventories is restricted to authorized personnel.

Physical Inventories are -

- supervised by someone independent of the custodial or record keeping functions.
- made by or tested by employees independent of the department being inventoried.
- recorded on permanent inventory count sheets.

Inventory

Example Key Controls (Continued)

- re-recorded on count sheets signed and dated by the person supervising the count.
- planned to provide provisions for cut-off of receipts and issues.
- reflected in the perpetual records based on the actual inventory quantities.

Adjustments to inventory records are approved by a properly designated individual.

Physical inventory is taken at least annually.

Perpetual inventory balances are reconciled against the general ledger control accounts at least annually.

Management reviews perpetual inventory balance reconciliations at year-end.

Capital Assets

Example Objectives and Risks

Example Objectives	Example Risks
All capital asset transactions are initiated by authorized individuals in accordance with established criteria.	<ul style="list-style-type: none"> • Fictitious purchases or payments to contractors or suppliers, with or without kickbacks to employees. • Purchases from vendors whose interests are in conflict with the organization. • Purchases of unnecessary assets. • Disposal or scrapping of serviceable assets. • Purchases of assets which do not meet established quality standards.
Advance approval is obtained for all significant capital asset transactions.	<ul style="list-style-type: none"> • Unauthorized purchases, construction contracts or leases with companies, or individuals related to executive or legislative representatives. • Purchases from related parties without the knowledge of senior officials. • Delay or cancellation of a project. • Expenditures in excess of originally approved amounts without review and approval.
Adequate project cost records are maintained, and in-progress and completed project reports are issued.	<ul style="list-style-type: none"> • Actual costs that exceed projected amounts. • Overpayments to contractors. • Misclassification of costs between capital and operating budgets.

Capital Assets

Example Objectives and Risks (Continued)

Example Objectives	Example Risks
<p>All capital assets are accurately recorded in detailed records which are compared with existing assets at reasonable intervals. All capital assets are adequately safeguarded.</p>	<ul style="list-style-type: none"> • Use of equipment or other assets for other than the unit of government's benefit. • Theft of tools and equipment, maintenance, or supply parts. • Payment of insurance on assets no longer owned. • Unauthorized disposals of assets or diverted proceeds from sales of assets. • Physical loss of assets through inadequate security or insurance coverage. • Continued ownership of obsolete or otherwise nonproductive assets. • Preparation of financial statements which do not accurately reflect existing assets.
<p>All capital assets transactions are properly accumulated, classified, and summarized in the general ledger accounts.</p>	<ul style="list-style-type: none"> • A misstatement of reported financial position and results of operations. • Violations of loan covenants and/or rules and regulations of various grantor agencies. • Financial or operational decisions based upon erroneous information.

Capital Assets

Minimum Internal Controls per the Accounting and Uniform Compliance Guidelines Manual for State and Quasi Agencies Chapter 8 – Capital Asset Accounting

Agency personnel are responsible for accountability for all assets under their control, including capital assets.

Adequate asset management staff should be assigned to recording and maintaining, on the PeopleSoft financial system, all capital assets meeting the capitalization threshold per the State of Indiana Capital Asset Policy.

Controls should be in effect to assure that additions, disposals, and transfers to other departments or agencies are recorded timely.

Inventories of capital assets should be performed each year in each department and compared to the PeopleSoft listing.

Results of inventories should be retained for audit purposes.

Capital assets with a cost less than the capital asset threshold per the State of Indiana Capital Asset Policy may be included in PeopleSoft Asset Management at the agency's option. All assets in the system should be capitalized.

Capital Assets

Example Key Controls

Capital asset system and control accounts are reconciled monthly.

Capital asset subsidiary accounts are reconciled to the capital asset control accounts monthly.

Property records are reconciled to property accounts at least annually.

Beginning balances, additions, disposals and ending balances reflected in the note disclosures are reconciled to the capital asset system.

Duties are segregated so that the following responsibilities performed by different people:

- Custodian of the capital assets and taking the annual inventory.
- Reconciliation of the Capital Asset System with the control accounts and making entries in the Capital Asset System.
- Custodian of the capital assets and tagging.
- Custodian of the capital assets and investigating the missing capital assets.
- Custodian of the capital assets, making entries in the Capital Asset System and making entries in the general ledger.

All asset purchases and receipts are approved by a designated person with proper authority.

All disposals of property are approved by a designated person with proper authority.

Changes to the fixed asset system are approved in advance by a designated person with proper authority.

Information Technology

Example Objectives and Risks

Example Objectives	Example Risks
Definition and communication of organizational structure, policies, and procedures.	<ul style="list-style-type: none"> • Control may be superficial, inconsistently followed, or subject to override or circumvention. • Segregation of incompatible duties. • Opportunities to perpetrate and conceal fraud may exist if personnel have direct or indirect access to assets.
Management and user involvement and approval.	<ul style="list-style-type: none"> • Personnel may not fully understand users' needs or the accounting aspects of the systems; systems may be developed that perform improper calculation, prepare erroneous reports, or cause other processing errors. • Systems may be designed with inadequate control in the application programs. • User control may be incomplete or ineffectual as a result of poor knowledge of the system and the processing functions performed by the application programs.
Restricted access to application system documentation.	<ul style="list-style-type: none"> • Unauthorized persons may obtain detailed knowledge of applications and use that knowledge to perpetrate irregularities.
Authorization and approval of systems changes.	<ul style="list-style-type: none"> • Personnel may make systems changes that do not conform to users' needs resulting in processing errors. • Unauthorized program modifications may be implemented to perpetrate and conceal fraud.

Information Technology

Example Objectives and Risks (Continued)

Example Objectives	Example Risks
Monitoring integrity of master files.	<ul style="list-style-type: none">• Master files may contain erroneous data that cause errors in all transactions using those data.• Master file data may be altered to allow the processing of fraudulent transactions.• Master file data may be altered prior to the preparation of statements or confirmation.
Verifying accuracy of output.	<ul style="list-style-type: none">• Unauthorized or fraudulent transactions introduced during processing may not be detected.

Information Technology

Minimum Internal Controls per the Accounting and Uniform Compliance Guidelines Manual for State and Quasi Agencies Chapter 2 – Internal Control

Management should design the entity'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.
- Audit Trails allow for sufficient documentation to trace all transactions from the original source of entry into the system, through all system processes, 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.

See also *Accounting and Uniform Compliance Guidelines for State and Quasi Agencies*, Chapter 14 – Information Technology Controls, in its entirety.

<https://www.in.gov/sboa/files/CH14-Information-Technology-Controls.pdf>

Information Technology

Example Key Controls

A formal documented security administration process is in place to ensure that all application access, including restricted access to financial applications, is approved.

Management periodically reviews monitoring reports to identify potential unauthorized activity.

The Disaster Recovery plan identifies the following –

- Critical applications.
- Staff responsibilities.
- Steps for recovery of the system.
- Computer equipment needed for temporary processing.
- Business location(s) that could be used to process critical applications in the event of an emergency.

The agency has taken steps to prevent and minimize potential damage and interruption through the use of data and program backup procedures, including off-site storage of backup data as well as environmental controls, staff training and hardware maintenance and management.

The agency monitors information systems access, investigates apparent violations, and takes appropriate remedial and disciplinary action.