

**STATE
OF
TENNESSEE**

**MANAGEMENT'S GUIDE TO
RISK MANAGEMENT
AND INTERNAL
CONTROL**



AUGUST 2007

***MANAGEMENT'S GUIDE TO RISK MANAGEMENT
AND INTERNAL CONTROL
Table of Contents***

Introduction

Overview

Instructions

Sections

I. Internal Environment

II. Objective Setting

III. Event Identification

IV. Risk Assessment

V. Risk Response

VI. Control Activities

Part 1 Strategic, Operations and Reporting Objectives

Part 2 Compliance

Part 3 Fraud

VII. Information and Communication

VIII. Monitoring

Report Requirements

Management Report

Report Checklist

Bibliography

INTRODUCTION

The complexity and diversity of today's global environment in both the private and public sectors has resulted in standards-setters and business groups together focusing on the importance of entity's assessing their approach to managing risks.

Risk management assessment helps management achieve the entity's goals and objectives and prevent loss of resources. Risk management also helps ensure effective reporting and compliance with laws and regulations, and helps avoid damage to the entity's reputation and associated consequences.

In addition, government interest in internal control and enhanced disclosure has grown as governments became more complex and as citizens demanded more accountability. This interest is supported by Tennessee's Governmental Accountability Act of 2002 (Tennessee Code Annotated, Section 9-4-56) which requires the preparation of strategic plans for Executive Branch agencies. The Legislative intent of the Act was to connect planning, budgeting, and accountability.

This heightened interest in risk management and accountability coincides with the state's Financial Integrity Act (FIA) provisions. The Financial Integrity Act (Tennessee Code Annotated, Section 9-18-102) requires that each agency of state government establish and maintain internal controls. Furthermore, that the head of each executive agency submit a letter acknowledging responsibility for maintaining the internal control system of the agency.

Since the Department of Finance & Administration published the original FIA guidance, new auditing standards issued by the American Institute of Certified Public Accountants (AICPA) relative to information systems controls (SAS 94) and communicating internal control deficiencies (SAS 112) became effective. In addition in 2004, the Committee of Sponsoring Organizations of the Treadway Commission (COSO) published *Enterprise Risk Management—Integrated Framework*, (COSO 2) which followed the widely accepted and utilized first COSO report *Internal Control—Integrated Framework* (COSO 1) published in 1994.

The Department of Finance & Administration, Division of Accounts, in consultation with the Comptroller of the Treasury, Division of State Audit, has revised the originally issued FIA guidance to ensure compliance with the requirements of FIA.

This revision replaces FIA guidance with an explanatory package of risk assessment tools, internal control checklists, and new reports reflecting the increased responsibility of top management. New requirements with respect to the internal control environment, risk management guidance, ethics requirements, compliance

with laws and regulations, and fraud risk management have been incorporated into the package entitled *Risk Management and Internal Control Requirements*.

The primary objective of this package is to educate agencies and departments regarding the importance placed on enterprise risk management and to provide examples of tools that may be used in efforts to effectively mitigate risk in each of its components. This guidance is meant to be used generally by all agencies recognizing that management will need to add agency-specific risks to each section and checklist; and, that the specific methodology and tools involved in its application and use will vary from agency to agency.

Each executive agency's responsibility for assessing risk and implementing internal control standards begins with the chief executive officer (commissioner) and extends to everyone in the agency. Each agency head personally holds the leadership responsibility for helping to design, implement, maintain, and champion an internal control program that encompasses all agency fiscal programs and related activities. Each agency's chief financial officer shares this leadership role, yet ultimate accountability remains with the agency head.

OVERVIEW

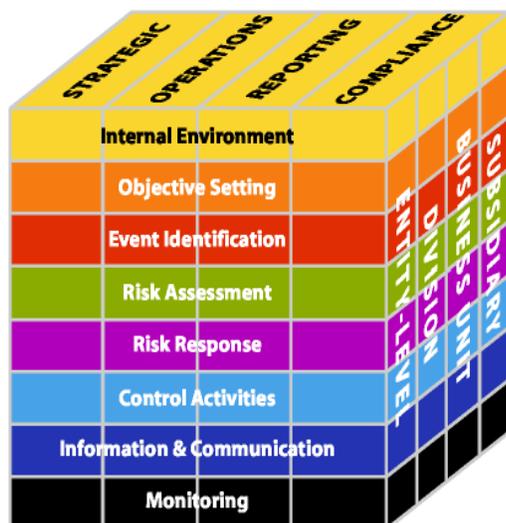
The guidance provided in this package is based on the two COSO reports discussed in the Introduction section. The frameworks identify and describe interrelated components necessary for effective internal control. Internal control is defined as a process, affected by an entity’s audit committee, board of directors, or other oversight body; management and other personnel; designed to provide reasonable assurance regarding the achievement of the following objectives categories:

Strategic—Effectiveness and efficiency of operations—Integrity and reliability of reporting—Compliance with applicable laws, rules, regulations, contracts, and grant agreements—Stewardship of assets.

Broader than Internal Control

Internal control is encompassed within and an integral part of enterprise risk management. Enterprise risk management is broader than internal control, expanding and elaborating on internal control to form a more robust conceptualization focusing more fully on risk. COSO 1 remains in place for entities and others looking at internal control by itself. Enterprise risk management is not strictly a serial process, where one component affects only the next. It is a multidirectional, iterative process in which almost any component can and does influence another.

Relationship of Objectives and Components



There is a direct relationship between objectives, which are what an entity strives to achieve, and enterprise risk management components, which represent what is needed to achieve them. The relationship is depicted in a three-dimensional matrix, in the form of a cube (known as the “COSO cube”).

The four objectives categories – strategic, operations, reporting, and compliance – are represented by the vertical columns, the eight components by horizontal rows, and an entity’s units by the third dimension. This depiction portrays the ability to focus on the entirety of an entity’s enterprise risk management, or by objectives category, component, entity unit, or any subset thereof.

Effectiveness

Determining whether an entity's enterprise risk management is "effective" is a judgment resulting from an assessment of whether the eight components are present and functioning effectively. Thus, the components are also criteria for effective enterprise risk management. For the components to be present and functioning properly there can be no significant deficiencies and material weaknesses, and risk needs to have been brought within the entity's risk appetite.

Testing the operating effectiveness of controls is different from obtaining evidence that controls have been implemented. When obtaining evidence of implementation by performing risk assessment procedures, management should determine that the relevant controls exist and that the entity is using them. When performing tests of controls, management should obtain evidence that controls operate effectively. This includes obtaining evidence about how controls were applied at relevant times during the period, the consistency with which they were applied, and by whom or by what means they were applied.

When enterprise risk management is determined to be effective in each of the four categories of objectives, respectively, audit committee, the board of directors, or other oversight body, and management have reasonable assurance that they understand the extent to which the entity's strategic and operations objectives are being achieved, and that the entity's reporting is reliable and applicable laws, rules, regulations, contracts, and grant agreements are being complied with.

Categories of Objectives

COSO 1 and COSO 2 specify three similar objectives categories – operations, reporting, and compliance. The reporting category in the internal control framework is defined as relating to the reliability of published financial statements. In the enterprise risk management framework, the reporting category is significantly expanded, to cover all reports developed by an entity, disseminated both internally and externally. These include reports used internally by management and those issued to external parties, including regulatory filings and reports to other stakeholders. In addition, the scope expands from financial statements to cover not just financial information more broadly, but non-financial information as well.

COSO 2 adds another category of objectives, namely, strategic objectives, which operate at a higher level than the others. Strategic objectives flow from an entity's mission or vision, and the operations, reporting, and compliance objectives should be aligned with them. Enterprise risk management is applied in strategy setting, as well as in working toward achievement of objectives in the other three categories.

COSO 2 introduces the concepts of risk appetite and risk tolerance. Risk

appetite is the broad-based amount of risk an entity is willing to accept in pursuit of its mission/vision. It serves as a guidepost in strategy setting and selection of related objectives. Risk tolerances are the acceptable levels of variation relative to achievement of objectives. In setting risk tolerances, management considers the relative importance of the related objectives and aligns risk tolerances with risk appetite. Operating within risk tolerances provides management greater assurance that the entity remains within its risk appetite, which, in turn, provides a higher degree of comfort that the entity will achieve its objectives.

Portfolio View

A concept not contemplated in COSO 1 is an enterprise-wide or aggregate view of risk. In addition to focusing on risk in considering achievement of entity objectives on an individual basis, it is necessary to consider composite risks from a “portfolio” perspective.

Components

With the enhanced focus on risk, COSO 2 expands COSO 1’s risk assessment component, creating four components: objective setting (which is a prerequisite to internal control), event identification, risk assessment, and risk response.

Internal Environment

In discussing the environment component, COSO 2 discusses an entity’s risk management philosophy, which is the set of shared beliefs and attitudes characterizing how an entity considers risks, reflecting its values and influencing its culture and operating style. As described above, the framework encompasses the concept of an entity’s risk appetite, which is supported by more specific risk tolerances.

Objective Setting

Objectives must exist before management can identify potential events affecting their achievement. Enterprise risk management ensures that management has in place a process to set objectives and that the chosen objectives support and align with the entity’s mission and are consistent with its risk appetite.

Event Identification

COSO 1 and 2 both acknowledge that risks occur at every level of the entity and result from a variety of internal and external factors. Both frameworks also consider risk identification in the context of the potential impact on the achievement of objectives.

COSO 2 discusses the concept of potential events, defining an event as an incident or occurrence emanating from internal or external sources that affect strategy implementation or achievement of objectives. Potential events with positive impact represent opportunities, while those with negative impact represent risks. Enterprise risk management involves identifying potential events using a combination of techniques that consider both past as well as emerging trends, and what triggers the events.

Risk Assessment

While both COSO 1 and 2 call for assessment of risk in terms of the likelihood that a given risk will occur and its potential impact, COSO 2 suggests viewing risk assessment through a sharper lens. Risks are considered on an inherent and a residual basis, preferably expressed in the same unit of measure established for the objectives to which the risks relate. Time horizons should be consistent with an entity's strategies and objectives, and, where possible, observable data. COSO 2 also calls attention to interrelated risks, describing how a single event may create multiple risks.

As noted above, enterprise risk management encompasses the need for management to develop an entity-level portfolio view. With managers responsible for programs, functions, processes, or other activities having developed a composite assessment of risk for individual units, entity-level management considers risk from a "portfolio" perspective.

Risk Response

COSO 2 identifies four categories of risk response – avoid, reduce, share, and accept. As part of enterprise risk management, management considers potential responses from these categories and considers these responses with the intent of achieving a residual risk level aligned with the entity's risk tolerances. Having considered responses to risk on an individual or a group basis, management considers the aggregate effect of its risk responses across the entity.

Control Activities

Both frameworks present control activities as helping ensure that management's risk responses are carried out. COSO 2 explicitly makes the point that in some instances control activities themselves serve as a risk response.

Information and Communication

COSO 2 expands on the information and communication component of internal control, highlighting consideration of data derived from past, present, and potential future events. Historical data allows the entity to track actual performance against targets, plans, and expectations, and provides insights into how the entity

performed in past periods under varying conditions. Present or current-state data provides important additional information, and data on potential future events and underlying factors completes the information analysis. The information system captures data in a timeframe and at a depth of detail consistent with the entity's need to identify events, assess and respond to risks, and remain within its risk appetite.

Monitoring

The entirety of enterprise risk management is monitored and modifications made as necessary. Monitoring is accomplished through ongoing management activities, separate evaluations, or both.

Roles and Responsibilities

Both frameworks focus attention on the roles and responsibilities of various parties that are a part of, or provide important information to, internal control and enterprise risk management. Everyone in an entity has some responsibility for enterprise risk management. COSO 2 describes the role and responsibilities of management and expands on the role of an entity's audit committee, board of directors, or other oversight body. A number of external parties often provide information useful in effecting enterprise risk management, but they are not responsible for the effectiveness of the entity's enterprise risk management.

Audit Committee, Board of Directors, or Other Oversight Body

The oversight body has a key role in the oversight of enterprise risk management and should discuss with senior management the state of the entity's enterprise risk management and provide oversight as needed. The oversight body should ensure it is apprised on a timely basis of the most significant risks, management's assessment, and the planned response to ensure effective enterprise risk management. Importantly, the oversight body should feel comfortable that appropriate processes are in place and that management is positioned to identify, assess, and respond to risk, and to bring relevant information to the oversight body level. The oversight body should consider seeking input from internal auditors, external auditors, and others. However, the oversight body should not consider the external auditors to be part of the entity's enterprise risk management.

Commissioner/Director/Department Head

The department head is ultimately responsible and should assume "ownership" for enterprise risk management. The department head's responsibilities include seeing that all components of enterprise risk management are in place (i.e., implemented). The department head generally fulfills these responsibilities by providing leadership and direction to senior managers and by setting broad-based policies reflecting the entity's risk management philosophy and risk appetite. The department head should assess the organization's enterprise risk management capabilities. The initial assessment should

determine whether there is a need for, and how to proceed with, a broader, more in-depth evaluation.

Senior Management

Management is directly responsible for all activities of an entity, including enterprise risk management. These responsibilities extend to compliance with laws, rules, regulations, contracts, and grant agreements applicable to the entity and its activities; the design and implementation of programs and controls to prevent and detect fraud; adopting sound accounting policies; establishing and maintaining effective internal control over financial reporting that will, among other things, initiate, record, process, and report transactions (as well as events and conditions) consistent with management's assertions embodied in the financial statements, including note disclosures; and testing the operating effectiveness of controls that management has determined are suitably designed to prevent or detect a material misstatement in a relevant financial statement assertion, a class of transactions, account balance, note disclosure, or material noncompliance.

Other Entity Personnel

Managers and other personnel should consider how they are conducting their responsibilities in light of this framework and discuss with more senior personnel ideas for strengthening enterprise risk management. Other managers support the risk management philosophy, promote compliance with the risk appetite, and manage risks within their spheres of responsibility consistent with risk tolerances. Other personnel are responsible for executing enterprise risk management in accordance with established directives and protocols.

Internal Auditors

Internal auditors should consider the breadth of their focus on enterprise risk management. Internal auditors can assist both management and the audit committee or other oversight body by examining, evaluating, reporting, and recommending improvements on the adequacy and effectiveness of management's risk management processes. COSO II provides a benchmark for internal auditors to use in the evaluation of their organization's risk management efforts. Also, internal auditors should consult the Institute of Internal Auditors Professional Guidance.

***INSTRUCTIONS
FOR
USING THE MANAGEMENT'S GUIDE
TO
RISK MANAGEMENT AND INTERNAL CONTROL***

The purpose of this guide is to assist agencies in the process of identifying, assessing and managing risks. Utilizing and applying the information contained herein will help ensure the adequacy of a complete risk assessment encompassing the components of the enterprise risk management framework as follows:

- I. Internal Environment
- II. Objective Setting
- III. Event Identification
- IV. Risk Assessment
- V. Risk Response
- VI. Control Activities
- VII. Information and Communication
- VIII. Monitoring

The stages of the risk assessment process have been outlined below and cross referenced to the related Sections of this Guide. It is important that internal and external sources of information be used throughout each stage, and, that appropriate communication channels be established within the agency throughout the evaluation process. See *Section VII, Information and Communication*, for further guidance.

The results of each of the following stages should be documented, in writing, to support the assertions made by management in the Management Report. Documentation should be maintained in the agency's office and available for review upon request. Several suggestions for documentation are made throughout this Guide.

Stage 1—Initial Assessment

Management should discuss and perform an in-depth evaluation of its entity's *Internal Environment, Objective Setting, Event Identification and Risk Assessment* (Sections I-IV) with key operating and financial personnel. The completion of this initial evaluation will provide the agency with a list of identified risks that would

interfere with the agency effectively and efficiently meeting any of its strategic, operations, reporting and compliance objectives. This initial evaluation should incorporate a likelihood-impact analysis for each risk identified (See Section II for a sample likelihood-impact matrix). The results of this evaluation will be applied to start the risk assessment process.

The results of the Sections I-IV evaluation may be documented in a manner that management deems appropriate. Several suggestions are made throughout this Guide. Additional examples, explanations and clarification can be found in the Application Techniques section of COSO 2. You are encouraged to incorporate these suggestions and examples into the chosen process.

Stage 2—Risk Assessment

Once management has performed an initial assessment using Sections I-IV of this Guide, the Risk Assessment in Section IV can be used to identify risks for Section VI. The inherent risks identified in Section VI of the Guide are a starting point and should be supplemented with risks identified during the initial assessment stage.

Stage 3—Control Activities

Section VI is designed to address inherent risks that are common in all agencies although many of the risks will not apply to some.

Management should supplement the worksheets in Section VI with agency-specific risks that have not been addressed in the sample worksheet. Any control activities identified as risk responses must be tested for effectiveness.

The intent of the control activities worksheet (Section VI) is to document responses to the inherent risks identified in achieving the entity's strategic, operations, reporting and compliance objectives. Also, the worksheet can be the vehicle to document the entity's consideration of the remaining risk, i.e., the residual risks, and the effectiveness of control activities. Management may utilize a different format to document its control activities as long as it includes the same information as Section VI.

Stage 4—Risk Response

Once management has addressed their identified risks with control activities (Section VI), all residual risks should be summarized and evaluated on an aggregate basis. The entity can then determine if the aggregate residual risks are within its risk tolerance.

Stage 5—Monitoring

Monitoring should be performed throughout the ordinary course of the entity's business. Refer to Section VIII of the Guide for guidance on the scope, frequency and documentation of monitoring activities. Evaluation tools provided in COSO 1 may serve as a useful reference for separate evaluations performed periodically.

Stage 6—Report Requirements

As a part of management's responsibility for assessing risk and implementing internal control standards, TCA § 9-18-104 requires certain reporting by the head of each agency. This should consist of a signed report to F&A and the Comptroller of the Treasury stating that a risk assessment has been performed, an effective system of internal control has been implemented to mitigate any significant deficiencies and material weaknesses, and internal controls are operating effectively. Please refer to the illustrative sample report at the end of the Guide.

In addition to submitting the Management Report and the Report Checklist, management should, at a minimum, submit a completed control activities evaluation that covers the primary objectives (strategic, operations, compliance, and reporting); the eight components, and the activities outlined in the control activities worksheet in Section VI.

SECTION I

INTERNAL ENVIRONMENT

The internal environment encompasses the tone of an organization, influencing the risk consciousness of its people, and is the basis for all other components of enterprise risk management, providing discipline and structure. Internal environment factors include an entity's risk management philosophy; its risk appetite; oversight by an audit committee; the integrity, ethical values, and competence of the entity's people; and the way management assigns authority and responsibility, and organizes and develops its people.

The following are elements of an effective internal environment and suggestions for consideration:

Risk Management Philosophy

An entity's risk management philosophy is the set of shared beliefs and attitudes characterizing how the entity considers risk in everything it does, from strategy development and implementation to its day-to-day activities. Its risk management philosophy reflects the entity's values, influencing its culture and operating style, and affects how enterprise risk management components are applied, including how risks are identified, the kinds of risks accepted, and how they are managed.

1. Has management's philosophy been developed, understood, and embraced by its personnel?
2. Has a method to monitor or test the attributes of management's philosophy been integrated into the entity's culture, e.g., a survey or other mechanism?

Management may articulate elements of their risk management philosophy in writing through policies or statements. To ascertain how well their philosophy is integrated into the entity's culture, a risk-related culture survey could be conducted. For example, a periodic survey might include questions under the following attributes—leadership and strategy, people and communication, accountability and reinforcement, risk management and infrastructure. The survey could require respondents to use a scale of -2 (strongly disagree, disagree) to +2 (strongly agree, agree) to answer questions such as “I understand the agency's overall mission and strategy” (under the leadership and strategy attribute) and “Disciplinary action is taken against those who engage in professional misconduct” (under the accountability and reinforcement attribute).

Risk Appetite

Risk appetite is the amount of risk, on a broad level, an entity is willing to accept in pursuit of value. It reflects the enterprise's risk management philosophy, and in turn influences the entity's culture and operating style.

1. Has risk appetite been considered in management's strategy setting?
2. Has risk appetite been considered in terms of the entity's stakeholders, e.g., the citizens?

Oversight by an Audit Committee

An entity's audit committee or other oversight body is a critical part of the internal environment and significantly influences its elements. The committee's independence from management, experience and stature of its members, extent of its involvement and scrutiny of activities, and appropriateness of its actions all play a role.

1. If an audit committee or other oversight body has been established, is it actively performing its oversight responsibilities?

Integrity and Ethical Values

The effectiveness of enterprise risk management cannot rise above the integrity and ethical values of the people who create, administer, and monitor entity activities.

1. Are the entity's Code of Ethics and other policies regarding acceptable business practice, conflicts of interest, and expected standards of ethical and moral behavior comprehensive and relevant?
2. Do employees fully and clearly understand what behavior is acceptable and unacceptable under the entity Code of Ethics and know what to do when they encounter improper behavior?
3. Are employees generally encouraged to "do the right thing" when faced with pressures to cut corners with regard to policies and procedures?
4. Does management take the appropriate remedial action when someone violates policies/procedures?

A code of conduct provides a connection between the organization's mission or vision and its operating policies and procedures. Not necessarily an exhaustive guide, a code of conduct is a proactive statement of an organization's positions on ethics and compliance issues. The following topics are often addressed in a code of conduct:

- Letter from chief executive—presents top management's message of the importance of integrity and ethics to the agency; introduces the code of conduct, its purpose and how to use it

- Goals and philosophy—considers the agency’s: culture, purpose, commitments to ethical leadership
- Conflicts of interest—addresses conflicts of interest and forms of self-dealing; speaks to personnel and other parties and those activities, investments, or interests that reflect on the agency’s integrity or reputation
- Gifts and gratuities—deals with giving of gifts and gratuities, setting forth the agency’s policy; sets standards and provides guidance regarding gifts and entertainment and their proper reporting
- Transparency—includes provisions dealing with the agency’s commitment to complete and understandable social, environmental, and economic reporting
- Agency resources—includes provisions dealing with agency and/or state resources, including intellectual property and proprietary information—whom these belong to and how they are safeguarded
- Social responsibility—includes the entity’s role as a government citizen, including its commitment to human rights, environmental sustainability, community involvement, and economic issues
- Additional conduct-related topics—includes provisions regarding adherence to policies established within specific areas, such as—employment issues; dealings with contractors, lobbyists, and economic issues; good faith and fair dealing with customers and suppliers; and confidentiality and security of information

Commitment to Competence

Competence reflects the knowledge and skills needed to perform assigned tasks. Management decides how well these tasks need to be accomplished, weighing the entity’s strategy and objectives against plans for their implementation and achievement.

1. Has management specified the competency levels for particular jobs and translated those levels into requisite knowledge and skills?

Organizational Structure

An entity’s organizational structure provides the framework to plan, execute, control, and monitor its activities. A relevant organizational structure includes defining key areas of authority and responsibility and establishing appropriate lines of reporting.

1. Is the internal audit function structured in a manner that achieves organizational objectivity and permits unrestricted access to top management and the audit committee?

Assignment of Authority and Responsibility

Assignment of authority and responsibility involves the degree to which individuals and teams are authorized and encouraged to use initiative to address issues and solve problems, as well as limits to their authority.

1. Have reporting relationships and authorization protocols, as well as policies that describe appropriate business practices, knowledge and experience of key personnel, and resources provided for carrying out duties been established?
2. Do all staff understand the entity's objectives, i.e., how their actions are related to one another and contribute to achievement of the objectives?

Human Resource Standards

Human resource practices pertaining to hiring, orientation, training, evaluating, counseling, promoting, compensating, and taking remedial actions send messages to employees regarding expected levels of integrity, ethical behavior, and competence.

1. Is consideration given to hiring the most qualified individuals, with emphasis on educational background, prior work experience, past accomplishments, and evidence of integrity and ethical behavior?
2. Have training policies been established that help personnel keep pace and deal effectively with the evolving environment?
3. Are integrity and ethics included in the criteria used to evaluate employees or division performance?

It is difficult to overstate the importance of an entity's internal environment and the impact—positive or negative—it can have on other enterprise risk management components. The impact of an ineffective internal environment can be far-reaching, possibly resulting in budgetary problems, a tarnished public image, or program failure. The attitude and concern of top management for effective enterprise risk management must be definitive and clear, and permeate the organization.

SECTION II ***OBJECTIVE SETTING***

Strategic objectives must exist before management can identify potential events affecting their achievement. Enterprise risk management ensures that management has in place a process to set strategic objectives and that the chosen objectives align with the entity's mission and are consistent with its risk appetite.

Strategic Objectives - Related/Selected Objectives

Objective Setting

- Is applied when management considers risks strategy in the setting of objectives
- Forms the risk appetite of the agency - a high-level view of how much risk management is willing to accept (objectives are set with regard to the risk appetite)
- Establishes a level of variation (risk tolerance), aligned with risk appetite, acceptable for objectives

Objective setting is a precondition to event identification, risk assessment, and risk response. There must first be objectives before management can identify and assess risks to their achievement and take the necessary actions to manage risks.

Within the context of an agency's established mission or vision, management should be establishing strategic objectives, selecting strategy, and setting aligned objectives cascading through the agency. The enterprise risk management framework is geared to achieving an entity's objectives, set forth in four categories:

- Strategic objectives – high-level goals, aligned with and supporting its mission
- Operations objectives – effective and efficient use of its resources
- Reporting objectives – reliability of reporting
- Compliance objectives – compliance with applicable laws, rules, regulations, contracts and grant agreements.

An objective in one category may overlap or support an objective in another.

In considering alternative ways to achieve its strategic objectives, management should identify the risks a range of strategy choices and consider their implications. Various event identification and risk assessment techniques can be used in the strategy setting process. By focusing first on strategic objectives and strategy, an agency is then positioned to develop the related agency wide operations, reporting

and compliance objectives. Agency wide objectives are linked to and integrated with more specific objectives that cascade through the organization to sub-objectives for various activities.

Objectives need to be readily understood and measurable. Enterprise risk management requires that personnel at all levels have an understanding of the agency's objectives as they relate to their role. They must have an understanding of what is to be accomplished, and a means of measuring what is accomplished.

Effective enterprise risk management does not dictate which objectives management should choose, but that management has a process that aligns strategic objectives with the agency's mission and that ensures the chosen strategic and related objectives are consistent with the agency's risk appetite.

Risk Appetite

Risk appetite, established by management, is a guidepost in strategy setting. Usually any number of different strategies can be designed to achieve desired goals, each having different risks. Management should align the organization, people, processes, and infrastructure to facilitate successful strategy implementation and enable the entity to stay within its risk appetite.

Defining the organization's risk appetite is an executive responsibility. It is undertaken in conjunction with evaluating alternative strategies in pursuit of the agency's goals and objectives. Management assesses the alternatives, sets objectives aligned with strategy, develops business processes to accomplish the plan, and manages any inherent risks. Risk appetite can be expressed as impact (potential consequences of a risk-based event), likelihood of a risk's occurrence, and associated mitigating actions.

Risk Tolerance

Risk tolerances are the acceptable level of variation relative to the achievement of objectives. In setting risk tolerances, management considers the relative importance and priority of the related objectives, and aligns risk tolerances with risk appetite.

Both risk appetite and risk tolerance set boundaries of how much risk an entity is prepared to accept. Risk appetite is a higher level statement that considers broadly the levels of risks that management deems acceptable while risk tolerances are narrower and set the acceptable level of variation around objectives. Operating within risk tolerances provides management greater assurance that the company remains within its risk appetite, which, in turn, provides a higher degree of comfort that the agency will achieve its objectives.

The following methods may be used to document the objective setting process:

Strategic Objectives:

List the agency's high-level goals that have been aligned with and support the agency's mission/vision. These are the objectives that should reflect management's choice as to how the agency seeks to create value for its stakeholders. For each objective briefly summarize other options and the reasoning underlying its selection.

Related Objectives:

For each strategic objective, list the operations, reporting and compliance objectives, as well as the related sub objectives, in a manner that clearly illustrates how the objectives are linked and integrated.

AGENCY MISSION/VISION	
STRATEGIC OBJECTIVES	1) 2)
STRATEGIES	1) 2) 3)
DIVISION #1 OBJECTIVES	1) 2) 3) 4)
DIVISION #2 OBJECTIVES	1) 2) 3) 4)

Risk Appetite:

Document the risk appetite, established by management that has been used as a guidepost in strategy setting in either qualitative or quantitative terms.

One approach is the likelihood-impact assessment. According to this approach, for each risk the frequency of occurrence (likelihood) and the worst credible outcome (impact) are assessed and captured in a likelihood-impact matrix. The matrix is then compared with a risk appetite map, which outlines the maximum level of adverse risk outcome that an agency is willing to accept.

As a result of this comparison, any significant risk exceeding the risk appetite will call for management action. The matrix helps with risk assessment and provides a visual representation of risk.

IMPACT	<u>HIGH</u>			EXCEEDING RISK APPETITE
	<u>MEDIUM</u>			
	<u>LOW</u>	WITHIN RISK APPETITE		
		<u>LOW</u>	<u>MEDIUM</u>	<u>HIGH</u>
		LIKELIHOOD		

Risk Tolerances:

The acceptable levels of variation relative to the achievement of objectives are often best measured in the same units as the related objectives. Documenting and defining acceptable levels of variation can be made part of the objective listing processes.

The below example is provided to help clarify the difference between risk appetite and risk tolerances:

An information providing agency decides to enter the e-commerce marketplace but has a low risk tolerance relative to its relationship with existing customers, particularly with respect to providing requested information promptly and accurately. To protect these relationships, management allocates necessary resources (people,

processes, technology) to ensure that 1.) request-to-information provision response times meet or exceed defined targets, and 2.) the accuracy of the information provided meets or exceeds defined criteria.

Management is now conducting business online and has installed the resources needed to protect its reputation for timely and accurate provision of requested information. It has set a target for delivery within three days of accepting requests and has guaranteed delivery within one week by a statement on its Web site. However, how much variation is management willing to tolerate with respect to delivery and information accuracy targets? Is a two-day average variance around the delivery target too much (based on the value placed at risk [customer relationship])? The delivery targets and level of variation around these are the risk tolerances.

SECTION III ***EVENT IDENTIFICATION***

Event identification represents a critical step in enterprise risk management. Failure to identify possible risk events will likely result in an incomplete risk universe. Management must identify events affecting an agency's ability to successfully achieve its objectives, distinguishing between risks and opportunities. The opportunities then need to be channeled back to management's objective-setting process. Events with a potentially negative impact represent risks, which require management's assessment and response.

Factors Influencing Strategy and Objectives

Enterprise risk management focuses on risks to the achievement of all business objectives, not just the financial statement assertions. Event identification therefore involves a cross-section of management, as possible events include business scenarios of which financial management may not be aware. Key steps to achieving event identification objectives include examining each business objective with relevant managers via facilitated risk event (scenario) exercises, and evaluating event-scenario drivers to determine interdependencies and interrelationships. Because events do not occur in isolation, management needs to understand how events interrelate. By assessing interrelationships, a determination of where risk management efforts are best directed can be made.

Simply put, event identification is a process of systematically recognizing potential events that affect the achievement of business objectives. An event is an incident or occurrence resulting from internal or external sources that affects the implementation of a strategy or achievement of objectives. Events may have a positive or negative impact, or both. (Even events with a relatively low probability of occurrence should not be ignored if the impact on achieving an important objective is great.)

Methodologies and Techniques - Risks and Opportunities

Identifying the external and internal factors that influence events is useful to effective event identification. Once the major contributing factors are identified, management can consider their significance and focus on events that can affect achievement of objectives.

Examples of external and internal factors:

External
Economic
Natural environment
Political
Social

Internal
Infrastructure
Personnel (people/culture)
Processes
Technology (systems)

Technological

An agency's event identification methodology may comprise a combination of techniques, together with supporting tools; and, looks to both the past and the future.

Examples of techniques for identifying events:

- Event inventories (listing common potential events)
- Internal analysis (completed as part of a routine planning cycle process, typically through staff meetings)
- Escalation or threshold triggers (compare current transactions or events with predefined criteria)
- Facilitated workshops and interviews (draw on accumulated knowledge and experience of management, staff and stakeholders through structure discussions)

The above techniques are typically applied in particular circumstances, with varying frequency over time. Potential events are also identified on an ongoing basis in connection with routine business activities, such as (a) industry/technical conferences, (b) peer websites, (c) benchmarking reports, (d) industry, trade and professional journals, (e) media reports, and (f) monthly management reports.

Because of the potential for forgetting risks, agencies may want to create risk categories to assist in the identification process. Another useful tool is to introduce an intermediate step - identifying what you depend upon to achieve your objectives. This is sometimes much easier than trying to think about all the events that could prevent success. (For example, if the objective is to get to work on time, it is easy to list the dependencies, i.e. alarm clock to wake you up, car to take you to the bus station, bus to take you into town. The next step is to list, in a structured way, the known events that could jeopardize your objective, i.e. alarm clock could fail to go off due to a power outage; the car could have a flat tire or the bus is running late.)

Remembering that an "event" is anything that prevents the achievement of an objective as planned, whether it is a "good" event or a "bad" event, consideration should be given to the following:

- Does my agency have processes in place to identify (and document) those incidents occurring internally or externally, that could affect the strategy and achievement of objectives (for example, unexpected employee turnover, a tornado or unexpected reduction in federal levels of funds)?
- Are these processes systematic and ongoing? Do they incorporate the use of "what-if" and "worst-case" scenarios?
- Do these processes cover all types of objectives (i.e. strategic, operational, compliance and reporting)? Exhibit A provides an example of a Risk

Identification Template that may be helpful in ensuring that all events, both financial and non financial in nature are considered.

- Do these processes consider potential threats to and vulnerabilities in the information system or business processes as a result of threat types such as system failures, cyber crime, virus/worms, hackers, and spy ware?
- Do these processes consider event interdependencies? In other words, are the risk events isolated, are they part of a chain reaction, or do they result in ripple effects?

RISK IDENTIFICATION TEMPLATE

Each individual of the organizational or operating units is given a template with instructions to list the key strategies and/or objectives within his or her area of responsibility and the risks that could impede the achievement of the objectives.

Please list the major strategies and/or objectives for your area of responsibility/unit.

Please list the major risks your unit faces in achieving your objectives.

Please assess the overall risk management capability within your area of responsibility to seize opportunities and manage the risks you have identified.

SECTION IV ***RISK ASSESSMENT***

During the risk assessment process risks are analyzed and assessed as to their likelihood and impact. This allows an agency to consider the impact on the achievement of agency objectives. Both qualitative and quantitative methods are typically used.

Strategic, Operational, Reporting and Compliance Objectives

In risk assessment, management considers the mix of potential future events – both the expected and unexpected events. Many events are routine and recurring; and management has already addressed potential risk in on-going reporting, controls, corrective action, etc. In risk assessment, management assesses the risk of unexpected potential events, and considers expected events that have not already been reviewed.

A useful first step is typically a brainstorming session among appropriate division/unit managers and employees. Steps should include reviewing whether appropriate policies and procedures are in place, recent audit findings, significant deficiencies or material weaknesses, and possible opportunities of management override of controls. Often it is helpful to ask, “What is the worst thing that could happen; what is the worst thing that has happened?”

Understanding “Risk Appetite”

In the process of risk assessment, an agency should consider its “risk appetite,” broadly defined as the amount of risk that an entity is willing to accept in pursuing its objectives. Risk appetite directly influences the agency’s culture and operating style. For most governmental entities, whose functions are defined by law, regulation, and budget appropriation, the risk appetite of a given agency would be fairly low. In the COSO II enterprise risk framework, risk tolerance, a more familiar term, relates to the tolerable level of variation associated with a particular objective.

Risk Assessment - A Daily Responsibility

While conducting risk assessment is typically considered a “one time activity,” in the context of enterprise risk management it is continuous and on-going, part of the daily responsibility of managers and employees throughout the organization.

Inherent and Residual Risk

The risk assessment process considers both inherent and residual risk. Inherent risk is risk absent any management activity or controls to prevent an event from happening.

Residual risk is the level of risk that remains after management has a plan in place to deal with the risk.

Example: An agency sets up a payment card program to purchase certain goods and services. Inherent risk is mitigated by the program's policies and procedures, while residual risk remains after those policies and procedures are in place.

Likelihood and Impact

Managers should consider both the likelihood and impact of potential risks. Likelihood represents the possibility an event will occur, impact represents its effect on the agency and others. Often likelihood is informally quantified as "low, medium, or high" or through a percentage, frequency of occurrence, or some other measure.

Qualitative and Quantitative Methods

Typically an entity's risk assessment method includes both qualitative and quantitative methods. While quantitative methods bring more precision, qualitative methods are appropriate in situations in which the business process or program activity does not lend itself to quantitative analysis, nor is it cost-effective to do so. The choice of methods should reflect the needs of the business unit, and the culture of the business unit and its employees.

Example: "In one company... .. in identifying and assessing risk at a process level, one business unit uses self-assessment questionnaires while another uses workshops. The risks are assessed on an inherent and a residual basis, and then organized and grouped by risk categories and objectives for both business units. Although different methods are used, they provide sufficient consistency to facilitate assessment of risks across the entity." (COSO II, page 53).

Overlap in Risk Categories

Typically there is considerable overlap of specific risks among the COSO II risk categories. For example, the second example of operational failure listed below - families in need not receiving benefits in a timely fashion - also results from a lack of compliance with regulation. And the example used in the compliance section - failure to follow the court-ordered instructions - could have definite strategic consequences. The following are examples of risk categories:

	Specific Risks	Risk Assessment
Strategic	The agency fails in its basic requirement to provide services as defined by T.C.A.	The assessment notes the type of event that would cause this to occur, tracks the on the population, environment, etc.with appropriate data and statistical information. notes risk after management’s intervention and the corrective action plan.
Operational	Departmental personnel disregard state purchasing policies when making small dollar purchases.	Failure to follow purchasing policies may lead to employee purchase of inappropriate items, or fraud, waste or abuse, and failure to obtain the best price for state contracts.
	Food stamp clients meeting requirements for of “expedited services” are not properly identified, and thus do not receive benefits in a timely manner as required by federal regulation.	May result in sanctions and a penalty loss of funds. The assessment analyzes the risk of this occurring, # of expedited vs regular clients; staff available to meet expedited needs, and full impact of noncompliance.
	Subrecipients in HIV/AIDS programs are routinely reimbursed for unsupported expenditures	Extent of reimbursement and frequency is analyzed. Notes that paying subrecipients invoices for which no documentation exists and thus paying for services that may not have occurred subjects agency to worst possible fraud, waste, or abuse risk.

	Specific Risks	Risk Assessment
	Agency equipment records are not accurate. Key management officials have disregarded the need for information on equipment.	Extent of problem is analyzed through samples or surveys. When the reason for the breakdown in the process is apparent disregard of information by key officials, the problems are more serious than flaws in control design.
Reporting	Management did not notify the Comptroller of the Treasury of overpayments totaling \$\$-----. No attempt made to recover funds.	Assess why there was a breakdown both in state's policy and in actual recoupment of overpayment. Lack of notification of the Comptroller's Office negates possibility of a thorough investigation.
	Accounts Receivable were maintained in Policy 23— an off-line spreadsheet.	Assess lack of compliance with(receivables) and impact of failure to record receivables in State's accounting system, and impact on collection and write-off.
Compliance	Agency did not follow court-ordered instructions and standards on service delivery.	Assess reason for non-compliance, individual responsible for failure, lack of management oversight, etc. May result in further court oversight.

SECTION V ***RISK RESPONSE***

Having assessed relevant risks, management determines how it will respond, reviewing likelihood and impact, evaluating costs and benefits of responses, and selecting options that bring residual (remaining) risk within the entity's risk tolerances.

The Four Categories of Risk Response

In responding to identified risks, there are four basic ways to respond:

- *Avoidance*: Exiting or not participating in the activities that give rise to risk, such as declining expansion or not undertaking a new initiative.
- *Reduction*: Specific actions taken to reduce the likelihood or impact of a risk, or both. This is the most usual risk response for governmental entities.
- *Sharing*: Reducing the likelihood of risk by sharing a portion of the risk with other entities, such as purchasing insurance.
- *Acceptance*: No action is taken, and the entity learns "how to live with the risk."

Additional Factors in Risk Response

For many risks, appropriate responses are obvious and well accepted. In determining risk responses, management should consider such things as:

- Effects of potential responses on risk likelihood and impact. A response to risk may affect likelihood and impact differently.
- Cost versus benefits of potential responses. Generally it is easier to deal with the cost side of the equation, which often can be quantified. The benefit side may involve more subjective valuation.
- Possible opportunities to achieve entity objectives going beyond dealing with the specific risk. A response to a given risk may lead to improvements in other services areas.

A Portfolio or Entity-Wide Perspective

The enterprise risk management approach requires that risk be considered from a "portfolio," or entity-wide perspective. Management first determines risk in each division or business unit, with the responsible manager developing a composite assessment of risk for the unit reflecting the unit's residual risk profile relative to its objectives and risk tolerances.

A portfolio view of risk can be depicted in a variety of ways, focusing on major risk or event categories across divisions, business, or program units. While risks in particular units may be within risk tolerances of those units, taken together they may exceed the risk appetite of the entity as a whole or may have common elements, in which case additional risk response steps may be necessary.

Several examples of risks previously identified are provided below:

	Specific Risks	Risk Response
Strategic	The agency fails in its basic requirement to provide services as defined by T.C.A.	For a broad and significant risk, management typically reviews a range of responses; requiring further investigation and analysis, possibly establishing a high-level work team to delineate options, address cost versus benefit, and establish a corrective action plan.
Operational	Departmental personnel disregard state purchasing policies when making small dollar purchases.	Corrective action plan requires compliance with purchasing policy and procedures, may include retraining, monitoring of purchasing activity to ensure compliance and appropriate residual risk.
	Food stamp clients meeting requirements for “expedited services” are not properly identified, and thus do not receive benefits in a timely manner as required by federal regulation.	After assessment and additional data, corrective action plan may include work team to develop additional training, additional methods to identify and monitor progress of expedited cases —within cost/benefit framework.

	Specific Risks	Risk Response
	Subrecipients in HIV/AIDS programs are routinely reimbursed for unsupported expenditures	After further analysis, corrective action plan identifies and remedies failures in the reimbursement process, cost/effective methodology to monitor.
	Agency equipment records are not accurate. Key management officials have disregarded the need for information have disregarded the need for information on equipment.	Corrective action plan identifies responsibility for record-keeping. Reviews with management key role in avoiding loss of state assets.
Reporting	Management did not notify the Comptroller of the Treasury of overpayment of \$\$---- and failed to recoup overpaid funds.	Corrective action plan requires compliance and retains staff in Policy 11. Reviews recoupment procedures to be followed.
	Accounts Receivable were maintained in off line spreadsheet.	Corrective action plan addresses non-compliance with Policy 23, consults with Accounts.
Compliance	Lack of compliance with federal regulations led to legal action by plaintiffs, court ordered reporting and monitoring.	Corrective action plan sets up blue-ribbon team, reporting to agency chief executive, and authorized to initiate program steps necessary to eventually eliminate court oversight.

SECTION VI

CONTROL ACTIVITIES

Control Activities are the policies and procedures that help to ensure that management's risk responses are carried out. Control activities occur throughout the organization, at all levels and in all functions. They include a range of activities - as diverse as approvals, authorizations, verifications, reconciliations, reviews of operating performance, security of assets, and segregation of duties.

Control activities may function to ensure risk responses are carried out as well as perform as risk responses with respect to certain objectives. These checklists are designed to enable an organization to integrate control activities with risk responses.

Control activities sometimes include a policy in place to ensure the objectives are met and in addition, procedures to effect the policy. The policies in place to ensure objectives are met should be addressed in Parts I and III and the activities to ensure compliance with those policies should be addressed in Part II. Any policies identified as a control activity in Part I or Part III should be added to the list in Part II if it functions as a control activity.

General and application system controls may be used to address any of the risks identified in any of the parts and not just under the information systems components of this section.

Given the wide variety of organizational objectives across State agencies, it would be impossible for this tool to address all possible risks. This list is a starting-point and is not designed to be all-inclusive. By using the other tools contained in the other sections of this manual, agency personnel should closely evaluate its agency's internal environment, objectives, and identified events to ensure all risks have been identified. Additional risks identified by the agency should be addressed at the end of each category. It is acceptable for a control to be in place to mitigate more than one identified risk.

SECTION VI CONTROL ACTIVITIES

Part 1 Strategic, Operations and Reporting Objectives

Objective: Respond to the identified inherent risks to the organization's Strategic, Operations and Reporting objectives in order to determine the residual risks. Determine the effectiveness of those control activities.

1. Address the following risks and add any identified agency-specific risks.
2. For each risk, estimate the potential impact to the agency assuming the risk occurs. Use High, Medium or Small.
3. For each risk, assess the likelihood of the risk occurring. Use Probably, Reasonably Possible or Remote. Alternatively, use High, Medium or Low.
4. For each risk with large or moderate impact and probable (high) or reasonably possible (medium) likelihood of occurrence, list the control activity to mitigate the risk to an acceptable level. If no control activity is present to manage the risk, a corrective action plan should be completed and attached. Any N/As should be explained.

Fraud Risks are identified in Part III of this section.

Objective Category	Risk and Exposure	Impact	Likelihood	Control Activity	Control Operating Effectively?
1. BUDGET					
Strategic	Budget does not provide for adequate funding to meet the agency's mission, goals and objectives.			<i>Example: Significant/material programs/activities are prioritized to ensure the agency's mission, goals, objectives are met.</i>	
Operations	Agency failed to operate efficiently within their budgeted parameters.			<i>Example: Significant/material programs/activities are prioritized to ensure the agency's mission, goals, objectives are met.</i>	
	Budget not prepared timely.			<i>Example: Agency prepares budget calendar.</i>	
	Finance and Administration not informed in time of expenditures in excess of appropriations or the budget.			<i>Example: IS controls are in place to prevent overspending the legal level of budgetary authority.</i>	

Objective Category	Risk and Exposure	Impact	Likelihood	Control Activity	Control Operating Effectively?
	Agency failed to fulfill their legislative mandates.				
	Budget fails to provide effective management and cost control.			<i>Example: Management periodically reviews budget position with YTD expenditures. System rejects expenditures that are over budget.</i>	
	Unexpected cut in federal funding.			<i>Example: Revenue estimates are based on prior year amounts as well as identified contingencies.</i>	
	Unexpected decline in revenue collections.				
	Unexpected increase in expenditure requirements due to unforeseen casualty losses.				
Reporting	Expenditures are not recorded to the proper budget control account/allotment code.				
	Appropriations are not recorded to the proper budget control account/allotment				
	Additional Risks and Exposures	Impact	Likelihood	Additional Control Activities	Control Operating Effectively?
2. CASH DISBURSEMENTS/EXPENDITURES					
Strategic	Ineffective management of cash outflows results in the lack of maximization of State resources.				

Objective Category	Risk and Exposure	Impact	Likelihood	Control Activity	Control Operating Effectively?
Operations	Expenditure not recorded against proper purchase order or contract.			<i>Example: Outstanding purchase orders are reviewed and status documented.</i>	
	Cash disbursement exceeds invoice amounts.			<i>Example: Someone independent of payable function reviews cash disbursements against supporting documentation and documents review.</i>	
	Agency pays for insufficient goods/services.			<i>Example: Payment is not authorized until receiving reports are matched against purchase order, invoice, and packing slip.</i>	
	Due to untimely payment, agency incurs late fees.				
	Agency pays for goods and services beyond vendor's quotes.			<i>Example: Vendor estimates are compared and attached to invoices.</i>	
	Agency fails to collect on cash advances.			<i>Example: Cash advances are recorded as receivable in system and A/R collection procedures are applied to cash advances.</i>	
	Subrecipients are not reimbursed timely causing a financial burden for the subrecipient.				
	Agency pays for goods not ordered.				
	Agency overspends grant award.			<i>Example: F&A policy 20 implemented and a schedule of grant awards and total expenditures is maintained and a review is documented periodically.</i>	
Reporting	Outgoing cash flow is recorded in wrong period.			<i>Example: Appropriate cut-off procedures are established and periodically reviewed.</i>	
	Expenditures not recorded in proper fund.				
	Expenditure not recorded under proper financial statement function.			<i>Example: An independent review of processed transaction details is performed and documented to check for proper coding of transactions.</i>	
	Claimant submits claim for reimbursement twice and both claims are paid by agency.			<i>Example: IS application control prevents duplicate payments and override of controls without prior manager approval.</i>	

Objective Category	Risk and Exposure	Impact	Likelihood	Control Activity	Control Operating Effectively?
	Vendor invoices received prior to month-end are incorrectly recognized as an expenditure in the following year.				
	Vendors are paid from statements as well as invoices, resulting in duplicate payments.			<i>Example: IS application control matches statements and invoices for similar amounts due and produces an exception report that must be reviewed by a supervisor before authorization for payment is permitted.</i>	
	Invoices are not marked paid resulting in duplicate payments.			<i>Example: All invoices are stamped "paid" with check number and date.</i>	
	Expired or unnecessary encumbrances remain on the books due to uncanceled purchase orders.			<i>Example: All encumbrances at year-end are reviewed for propriety.</i>	
	Expenditures incurred through the petty cash fund are not recorded as expenditures in accounting system before year end.				
	A manual check is not recorded in the system.			<i>Example: All checks numbers and amounts recorded in the system are matched up against the check registers with a check log created and initialed by reviewer on a weekly basis.</i>	

Objective Category	Risk and Exposure	Impact	Likelihood	Control Activity	Control Operating Effectively?
	Requisitions are not encumbered at year-end under modified accrual funds.				
	Expenditures are not recorded in accordance with GAAP due to inadequately trained accounting personnel.			<i>Example: Accounting personnel are required to attend a certain number of hours of training every year.</i>	
	Indirect costs are not posted to accounting records when drawdowns are made.				
	Additional Risks and Exposures	Impact	Likelihood	Additional Control Activities	Control Operating Effectively?
3. CASH RECEIPTS/REVENUES					
Strategic	Cash/Revenue collection efforts are inadequate to fund the agency's missions.				
Operations	Agency fails to earn adequate interest on cash deposits.			<i>Example: All accounts are interest bearing and all deposits of \$100.00 or more are made daily and every three days if less than \$100.00.</i>	
	Bank fails to credit agency's bank account properly.				
	Federal drawdowns are made late.				
	Agency fails to bill for all services rendered.				

Objective Category	Risk and Exposure	Impact	Likelihood	Control Activity	Control Operating Effectively?
	Customer billings fail to cover costs incurred.			<i>Example: Management compares expenditures incurred for an organization against revenue collections and monitors and documents on a monthly basis.</i>	
	Agency is not reimbursed for federal expenditures incurred due to late reimbursement request.				
	Agency is not reimbursed for federal expenditures due to lack of drawdown request.				
	Federal Funds are drawn before the Federal disbursements are made.				
	Cash is not deposited in the bank in a timely manner causing the agency to lose potential investment income.			<i>Example: All deposits are made in accordance with F&A policy 25.</i>	
Reporting	Revenues are recorded before earned.			<i>Example: Management assesses/analyzes revenues to ensure that the earnings process is substantially complete.</i>	
	Revenues are recorded before available and measurable under modified accrual funds.				
	Revenue recorded in customer database does not match actual payment made by customer.				
	Revenues recorded in system do not match amounts deposited or received.			<i>Example: Cash receipts issued numerically are all accounted for in the accounting system and reconciled with daily deposits. In addition, total deposits are reconciled monthly on the bank reconciliation.</i>	
	Deposits are not recorded in the proper period.			<i>Example: A bank reconciliation is performed within 7 days of receipt of bank statement to ensure all deposits have been recorded in the system and before year end finalization.</i>	

Objective Category	Risk and Exposure	Impact	Likelihood	Control Activity	Control Operating Effectively?
	Revenue is recorded in incorrect revenue category.			<i>Example: Processed revenue transactions are reconciled with supporting documentation by batch.</i>	
	Revenue is not recorded in accordance with GAAP due to inadequate training of accounting personnel.				
	Agency is reimbursed for federal funds before expenditure is incurred resulting in unearned revenue recognition.			<i>Example: Expenditure supporting documentation is attached to any federal revenue/drawdown requesting documentation.</i>	
	Deferred revenue is not transferred to earned revenue in the period earned.			<i>Example: Deferred accounts are reconciled at year-end.</i>	
	Direct deposits are recorded in wrong period.				
	Person receiving cash fails to stamp check with agency's account number and check is deposited in wrong account.			<i>Example: Clerk making deposit verifies that checks have been stamped with restrictive endorsement.</i>	
	Check is lost in route to bank resulting in receipts not matching cash deposited.				
	Cash receipt clerk totals deposit slip incorrectly and bank records incorrect deposit amount.			<i>Example: Someone independent of the cash deposit preparation function creates a calculator tape of deposits and reconciles with deposit slip. The calculator tape is attached to agency copy of deposit slip with copies of checks.</i>	
	Date cash received is not recorded on remittance support.			<i>Example: Cash receipt log is maintained with date as well as A/R information for back up support of cash receipts. Copies of checks are made at time of receipt.</i>	
	Excess cash collections are recorded as revenue instead of as a liability.				
	Additional Risks and Exposures	Impact	Likelihood	Additional Control Activities	Control Operating Effectively?

Objective Category	Risk and Exposure	Impact	Likelihood	Control Activity	Control Operating Effectively?
4. CASH MANAGEMENT					
Strategic	Inadequate cash on hand to support organization's mission/vision.				
Operations	An agency's uninsured/uncollateralized deposits with an insolvent depository are unrecoverable.			<i>Example: All of the agency's depositories are members of the State's collateral pool.</i>	
	An agency as a public depositor does not ensure that its title as a public depositor is listed on all bank accounts and certificate of deposits resulting in those deposits not qualifying for claim reimbursement from the collateral pool as a result of an insolvency of the depository.			<i>Example: Agency obtains acknowledgement from depository that funds are in agency's name and are classified as "public funds".</i>	
	Fund transfers to other bank accounts are not recorded in bank ledger resulting in insufficient funds upon a bank debit.			<i>Example: All bank transactions are accounted for during bank reconciliation. Non-check and deposit items are explained with internal form attached to the bank statement. Internal form includes ledger processing details and authorizing signature.</i>	
	Significant time lapse between drawdowns of funds from Treasury and actual receipt/recording of funds.				
	A returned check is not followed up on in a timely manner resulting in diminishing probability of collection.				

Objective Category	Risk and Exposure	Impact	Likelihood	Control Activity	Control Operating Effectively?
	Agency's checks have no void time frame printed on checks resulting in check remaining on outstanding check list for an excessively long amount of time or checks outstanding for a long period of time are not cancelled.				
Reporting	Fees charged by a financial institution are not reported in the financial records understating expenditures and overstating cash.				
	A certificate of deposit with an original maturity date of 24 months is incorrectly classified as cash equivalent.				
	An investment maturity automatically deposited in checking account is not properly recorded in accounting records.				
	A returned check is not recorded in the accounting records.			<i>Example: All NSF correspondence from bank is stamped with process date and initials of processor and copies are filed with bank statement, A/R and deposit files.</i>	
	Deposits made from a separate collection location is forwarded late to the main office and therefore not recorded in accounting records timely resulting in misstatement of cash on year end financial statements.				
	Additional Risks and Exposures	Impact	Likelihood	Additional Control Activities	Control Operating Effectively?

Objective Category	Risk and Exposure	Impact	Likelihood	Control Activity	Control Operating Effectively?
5. LIABILITIES					
Strategic	All payables, gains and loss contingencies and other liabilities are not properly accrued, reported, or disclosed.				
Operations	Sufficient funds are not available to liquidate liabilities.				
	The agency missed the opportunity to take advantage of discounts by remitting payment beyond the discount date due to late processing.				
Reporting	A liability for claims for losses that have been incurred and not reported are not accrued or measured using the measurement criteria in accordance with GASB 10.			<i>Example: An actuary is utilized for these types of claims.</i>	
	Accrued liabilities at fiscal year end are overstated in order to increase the level of expenditures in the next fiscal year				
	Vendor invoices received prior to month-end are not entered into the accounting records until the following year, understating liabilities at year end.			<i>Example: All invoices are date stamped with receipt date and all invoices received on last day of the accounting year are entered same day as received.</i>	
	Invoice amounts are recorded into accounting system for wrong amounts.			<i>Example: Transaction register total is reconciled with calculator tape of invoice totals.</i>	

Objective Category	Risk and Exposure	Impact	Likelihood	Control Activity	Control Operating Effectively?
	Calculations per vendor's invoice are incorrect but the total due was accrued as a liability and subsequently paid.			<i>Example: All vendor invoices are footed and crossfooted and initialed by A/P clerk.</i>	
	An invoice not belonging to the agency is entered into the accounting system.				
	Vendor credit advice is never received for goods that were returned.			<i>Example: Suspense file held by person independent of A/P function of all returns.</i>	
	Invoices received in numerous other locations are not sent to the processing office until after year end, understating liabilities.				
	Long term contract contractor's request for progress payments are accrued as liabilities even though they have yet to complete the first phase of construction.				
	Utility bills for the last month of the fiscal year not yet received prior to year end are not accrued but recognized as an expense in the following year.				
	Warrants are for an amount different than supporting invoices.				
	Compensated absences are not disclosed with the proper additions and reductions.				
	Additional Risks and Exposures	Impact	Likelihood	Additional Control Activities	Control Operating Effectively?

Objective Category	Risk and Exposure	Impact	Likelihood	Control Activity	Control Operating Effectively?
6. CAPITAL ASSETS/INVENTORY/EQUIPMENT					
Strategic	The agency is unable to adequately manage and account for their capital assets.				
Operations	Equipment is destroyed in a fire.				
	Interdepartmental transfer of equipment is not recorded.				
	Unsafe heavy work equipment causes an on-the-job injury.				
	Continuous maintenance needs of equipment causes numerous hours of lost productivity.				
	Asset cannot be located.			<i>Example: A 10% inventory is conducted quarterly and a 100% inventory is conducted annually of all assets.</i>	
	Management failed to send a completed inventory of office contents to Risk Management.				
	Agency is billed for telephone lines not utilized.				
	State agency fails to disconnect utilities at a location it has moved from and State continues to pay bills.				
Reporting	Project expenditures are not posted to the project file which tracks project year to date expenditures.			<i>Example: Project files are maintained with supporting documentation and reconciled with project status report periodically.</i>	
	Destroyed equipment/asset is not removed from accounting system.			<i>Example: A 10% inventory is conducted quarterly and a 100% inventory is conducted annually of all assets.</i>	

Objective Category	Risk and Exposure	Impact	Likelihood	Control Activity	Control Operating Effectively?
	Capital asset is not coded correctly at time of purchase resulting in expense of costs instead of capitalization.				
	Donated assets are not recorded in the capital assets or financial records.				
	Grant funded acquisitions are not tracked separately.				
	The agency does not hold title nor a lease agreement for land recorded on the books.				
	Capital asset acquisitions are not charged to federal grants but the depreciation is charged against the grant.			<i>Example: All depreciation charged to federal grants are recorded under tag number which is identified with the original acquisition transaction details and date charged to the federal government.</i>	
	Impairments in accordance with GASB 42 are not reported to the Division of Accounts.				
	Intangible assets are not identified as so and are expensed instead of capitalized in accordance with GASB 51.				
	Related accumulated depreciation is not removed from the records for disposals.				
	Additional Risks and Exposures	Impact	Likelihood	Additional Control Activities	Control Operating Effectively?

Objective Category	Risk and Exposure	Impact	Likelihood	Control Activity	Control Operating Effectively?
7. INFORMATION SYSTEMS/DATA PROCESSING					
Strategic	Computer system fails to generate reliable and/or accurate data.				
Operations	Untested and unaccepted programs are transferred into production.				
	Unauthorized changes are made to the computer system.				
	Technical support is inadequate to support agency's needs.				
	Fire and water damage destroy entire computer system with backup media stored at same location and as a result, all data is unrecoverable.			<i>Example: Backup media is stored in a separate building at least 10 miles from building where system resides.</i>	
	Computer system recovery after a natural disaster is significantly delayed due to outdated contact information of crucial personnel.				
	System recovery after a natural disaster is impeded as a result of information systems personnel being unaware of disaster recovery procedures and the Disaster Recovery Plans were stored in the same location as the system.			<i>Example: Disaster recovery plan is reviewed and an exercise of a mock disaster is performed by IS personnel annually. A copy of procedures are maintained by IS personnel at personal residence.</i>	
	Disaster Recovery Plan was never tested and fails in the recovery of the system after hardware and system failure.				
Reporting	System vendor information is unrecoverable after system failure.				
	Computer interfaces between general ledger systems do not operate to effect complete and accurate processing.			<i>Example: Divisions responsible for processing transactions are required to reconcile batch totals to documentation after every system interface.</i>	

Objective Category	Risk and Exposure	Impact	Likelihood	Control Activity	Control Operating Effectively?
	Rejected transactions are not identified and remedied resulting in unrecorded transactions.				
	Control tables are not updated with up to date tax rates.				
	Documents are input into system more than once resulting in duplicate transactions.			<i>Example: System edit checks include more than one invoice number, check number, etc.</i>	
	Input amounts do not agree with source documentation.			<i>Example: Documentation is totaled and batch total is documented on and compared with transaction register.</i>	
	Additional Risks and Exposures	Impact	Likelihood	Additional Control Activities	Control Operating Effectively?
8. PERSONNEL/EMPLOYEE COMPENSATION					
Strategic	Scheduled programs failed to run resulting in incomplete transaction processing and posting to accounting records.				
Operations	Poor management of personnel result in low morale and high turnover.				

Objective Category	Risk and Exposure	Impact	Likelihood	Control Activity	Control Operating Effectively?
	Payroll operations fail to provide for proper accounting and distribution of personnel pay.			<i>Example: All personnel are required to be paid via direct deposit to cut costs and prevent lost checks in the mail. Direct deposit data is sent back electronically from bank one day after payroll distribution to reconcile against payroll totals.</i>	
	Employees perceive limited control over their career development, causing higher turnover.				
	An employee is terminated for gross misconduct but receives payment for accrued leave anyway.				
	An employee continues to receive a salary payment after the employee's employment with the state has ended.				
	An employee is allowed to received a payroll differential after the reason for the differential has ended.				
	An employee is given a salary increase that was not authorized.				
	An employee is paid administrative leave without authorization.				
	An employee is paid compensatory time or overtime without prior approval.				
	Employee dissatisfaction with job variety results in rote performance, higher errors in key processes and high turnover.				
	Paychecks are distributed before the end of the payroll period.				
Reporting	Employees feel unrecognized, resulting in reduced focus on tasks and higher error rates.			<i>Example: Agency has an employee recognition program.</i>	

Objective Category	Risk and Exposure	Impact	Likelihood	Control Activity	Control Operating Effectively?
	Payroll deduction accounts in general ledger does not agree to subsidiary accounts balance.				
	Administrative leave accumulated and approved as discretionary leave is not accrued as part of the compensated absences liability.			<i>Example: Any administrative leave has to be taken before year-end or leave will be lost.</i>	
	Additional Risks and Exposures	Impact	Likelihood	Additional Control Activities	Control Operating Effectively?
9. FINANCIAL REPORTING					
Strategic	Processed transactions and procedures fail to timely provide data to compile financial statements that are accurate and reliable.				
Operations	The necessity of numerous offline adjustments causes the financial statements to be completed beyond a reasonable timeframe.			<i>Example: Offline adjustments must be justified in writing and approved in writing by management.</i>	
Reporting	The agency fails to properly adopt new accounting pronouncements due to uninformed and untrained personnel.				

Objective Category	Risk and Exposure	Impact	Likelihood	Control Activity	Control Operating Effectively?
	Fund balance is reserved and Net Assets are not restricted in accordance with statutory requirements.			<i>Example: Agency's reserve and restricted net assets requirements are all supported with TCA and reviewed annually for propriety and to determine if law has been updated.</i>	
	Financial statements do not articulate.				
	Agency fails to identify all of their reserve and restriction requirements.				
	Additional Risks and Exposures	Impact	Likelihood	Additional Control Activities	Control Operating Effectively?
10. ACCOUNTS RECEIVABLE					
Strategic	Recording and collection efforts are inadequate.				
Operations	Poor record management of receivables results in loss revenues and misstated receivables.				
	Collections are not applied to the correct customer account.			<i>Example: Statements are sent to customers monthly and any disputes are forwarded to someone independent of A/R function and documented thoroughly.</i>	
	Agency fails to follow up on interfund receivable for federal expenditures resulting in loss of federal funds due to time lapse.				
	Lack of collection efforts of delinquent receivables results in more write offs and loss of revenue.			<i>Example: Accounts delinquent more than 90 days are sent a collection letter and accounts older than 120 days are forwarded to collection agency.</i>	

Objective Category	Risk and Exposure	Impact	Likelihood	Control Activity	Control Operating Effectively?
Reporting	Cash collections unable to be identified with a subsidiary account.				
	Prior year's receivable reversal of a significant account is written off without adjusting the reversal.				
	A payment is recorded in a customer account but not deposited.				
	Receivables are reduced or written off without proper authorization.				
	Interest and fees are not calculated properly.			<i>Example: System calculates interest and fees</i>	
	Collections from separate collection site is not recorded into system due to untimely receipt by processing location.				
	The related estimated uncollectible account is not debited for a write off.				
	Additional Risks and Exposures	Impact	Likelihood	Additional Control Activities	Control Operating Effectively?
11. INVESTMENTS					
Strategic	Receivable account is erroneously credited for more than funds received.				
	Investment activity ensures solid safety, liquidity, accurate financial reporting and yield.				

Objective Category	Risk and Exposure	Impact	Likelihood	Control Activity	Control Operating Effectively?
Operations	Financial statements fail to portray actual investment balances and activity.				
	The U.S. interest rate changes by 50, 100 and 200 basis points (BPS) in next 12 months.			<i>Example: Investment policy requires diversity in investments other than investing assets heavily in one type, e.g. fixed income.</i>	
	Counter party in interest rate swap agreement exercises termination rights resulting in an adverse effect on the agency.				
	Investment personnel are unaware of future cash flow needs of the agency.				
	Income from investments are not credited to agency's broker/trustee account immediately when received.				
Reporting	Foreign currency in which investments are held are on a decline in relation to the U.S. dollar.				
	Stock investments are reported at cost.				
	Investment income is not posted by trustee/broker to agency's account statement which is the source documentation for entering investment income into accounting system.			<i>Example: Agency calculates interest income and compares to broker statements.</i>	
	Quoted market prices are not available for valuing derivatives resulting in the reliance on significant assumptions.				
	Investments are incorrectly valued on the financial statements due to lack of qualified accounting personnel.				
	Broker/Trustee miscalculates investment income.			<i>Example: Investment income is recalculated by agency investment system and compared to monthly statements.</i>	

Objective Category	Risk and Exposure	Impact	Likelihood	Control Activity	Control Operating Effectively?
	Reporting on derivative use is not in accordance with GAAP.				
	Additional Risks and Exposures	Impact	Likelihood	Additional Control Activities	Control Operating Effectively?

SECTION VI CONTROL ACTIVITIES

Part 2 Compliance

Objective: To identify mitigating controls that address the agency's risk of noncompliance with laws, rules, regulations, contracts, and grant agreements and to identify exposure for noncompliance. Determine the effectiveness of those control activities.

Instructions

1. Address the following risks and any identified agency-specific risks to the achievement of compliance with the related Law, Rule or Regulation.
2. For each risk, estimate the potential impact on compliance assuming the risk occurs. Use High, Medium or Small.
3. For each risk, assess the likelihood of the risk occurring. Use Probably, Reasonably Possible or Remote. Alternatively, use High, Medium or Low.
4. For each risk with large or moderate impact and probable (high) or reasonably possible (medium) likelihood of occurrence, list the control activity to mitigate the risk to an acceptable level. If no control activity is present to manage the risk, a corrective action plan should be completed and attached. Any N/As should be explained.

Law, Rule, Regulation, etc.	Risk or Exposure	Impact	Likelihood	Control Activity to Ensure Compliance Responsible Area?	Control Operating Effectively?
FEDERAL PROGRAMS					
<i>OMB Circular A-133</i>					
Activities Allowed/Allowable Costs	Costs charged to a federal program are not allowable under program regulations.				
Cash Management	The timing of federal cash draws are not in compliance with the Treasury-state agreement.				

Law, Rule, Regulation, etc.	Risk or Exposure	Impact	Likelihood	Control Activity to Ensure Compliance Responsible Area?	Control Operating Effectively?
	Program income is not disbursed before requesting additional federal cash draws.				
Davis-Bacon Act	Contractors and subcontractors are not informed of the requirements to comply with the Davis-Bacon Act.				
	Contractors and subcontractors under federal programs do not submit the required weekly certified payrolls.				
Eligibility	Recipients of federal grant funds do not meet eligibility requirements for the federal program.				
	Inadequate documentation is obtained from the federal program recipient to verify eligibility.				
	Benefits are not discontinued when the period of eligibility has expired.				
Equipment and Real Property Mgmt.	Use, management, and disposal of equipment and property acquired under a Federal grant is not in accordance with State laws and procedures.				
	Disposal of equipment acquired with federal dollars is made without the prior consent of the federal awarding agency.				

Law, Rule, Regulation, etc.	Risk or Exposure	Impact	Likelihood	Control Activity to Ensure Compliance Responsible Area?	Control Operating Effectively?
Matching, Level of Effort, Earmarking	Matching contributions for federal programs are funded with federal dollars.				
	Minimum or maximum limits for specified purposes are not met.				
Period of Availability	Federal funds are not expended within time frames specified in the federal award.				
	The agency fails to seek reimbursement during the specified funding period.				
Procurement, Suspension/Debarment	The department does not use the same State policies and procedures used for procurements from non-Federal funds.				
	Funds are disbursed to suspended or debarred parties.				
Program Income	Program income is not used according to requirements of the grant award.				
Relocation Assistance and Real Property Acquisition	Persons displaced by federally-assisted programs from their homes, businesses, or farms are not provided uniform and equitable treatment under the Uniform Relocation Assistance and Real Property Acquisition Policies Act of 1970, as amended.				

Law, Rule, Regulation, etc.	Risk or Exposure	Impact	Likelihood	Control Activity to Ensure Compliance Responsible Area?	Control Operating Effectively?
Reporting	All required federal reports are not submitted accurately and timely to the federal awarding agency.				
	Data presented in financial reports do not agree with accounting records.				
Subrecipient Monitoring	Subrecipients of federal awards are not monitored in accordance with the requirements of A-133.				
	Subrecipients are not informed of all grant requirements and provisions.				
	The agency fails to ensure that corrective action is taken on deficiencies noted during monitoring.				
Special Tests and Provisions	Noncompliance with the specific requirements that are unique to each Federal program and are found in the laws, regulations, compliance supplement, and the provisions of contract or grant agreements pertaining to the program.				
MISC. FEDERAL LAWS					
<i>Title VI of the Civil Rights Act of 1964</i>	The agency does not have a civil rights policy prohibiting discrimination.				

Law, Rule, Regulation, etc.	Risk or Exposure	Impact	Likelihood	Control Activity to Ensure Compliance Responsible Area?	Control Operating Effectively?
	Information about the agency's civil rights and affirmative action plan are not communicated or displayed through posters, brochures, etc.				
	The agency does not have published grievance procedures.				
	Grievance procedures are not distributed to employees.				
	There is not a designated compliance officer to handle complaints received.				
<i>Drug-Free Workplace Act</i>	The agency does not have and enforce a drug-free workplace policy.				
	There is not a tracking system in place to ensure that all employees have been issued and signed the policy.				
	There is not a designated compliance officer.				
<i>Health Insurance Portability and Accountability Act of 1996 . (HIPAA)</i>	Employees are not made aware of their responsibilities under HIPAA.				
	Unauthorized access is gained to records covered by HIPAA.				
	Improper disclosure of records covered by HIPAA is made.				

Law, Rule, Regulation, etc.	Risk or Exposure	Impact	Likelihood	Control Activity to Ensure Compliance Responsible Area?	Control Operating Effectively?
STATE LAWS AND RULES					
F&A Policy 1, <i>Automatic Deposit of Paychecks for New Employees</i>	Procedures are not in place to ensure that new employees are enrolled in direct deposit.				
F&A Policy 2, <i>Recovery of Monies, Refunds, Disallowances, and Questioned Costs</i>	Recoveries, refunds, disallowances, or return of questioned costs are not made in accordance with the provisions of Policy 2.				
F&A Policy 3, <i>Uniform Reporting Requirements and Cost Allocation Plans for Subrecipients Federal and State Grant Monies</i>	The department's cost allocation plan is not developed in accordance with the provisions of Policy 3.				
F&A Policy 4, <i>Recognition Versus Reduction of Amounts - Revenue, Expenditure Related Accounts</i>	Revenues and expenditures are not recorded in accordance with the provisions of Policy 4.				
F&A Policy 5, <i>Application of GASB Statement 3 - Deposits with Financial Institutions, Investments (including Repurchase Agreements), and Reverse Repurchase Agreements - and Application of GASB Statement 40 - Deposit and Investment Risks, An Amendment of Statement 3</i>	Financial statements are not prepared in accordance with GASB Statements 3 and 40, as outlined in Policy 5.				
F&A Policy 6, <i>Payments Under Contract After Closing or Purging of Contract From STARS</i>	Late contract payments are made without the proper approvals outlined in Policy 6.				

Law, Rule, Regulation, etc.	Risk or Exposure	Impact	Likelihood	Control Activity to Ensure Compliance Responsible Area?	Control Operating Effectively?
F&A Policy 7, <i>Petty Cash and Departmental Bank Accounts</i>	Unauthorized bank accounts or petty cash accounts are established.				
	Bank account reconciliations are not performed timely.				
F&A Policy 8, <i>Comprehensive State Travel Regulations</i>	An employee travels out-of-state without the proper approvals.				
	Travel advances are issued without the proper approval.				
	Travel claims are submitted and paid for travel that did not occur.				
F&A Policy 9, <i>Revenue Recognition of Taxes, Licenses, Permits and Fees on the Modified Accrual Basis</i>	Revenue recognition of taxes, licenses, permits, and fees is not made in accordance with the provisions of Policy 9.				
F&A Policy 10, <i>Dues and Subscriptions</i>	Initial membership dues and subscriptions exceeding \$1,000 are not approved by the Budget Division of the Department of Finance and Administration.				
	Renewals of membership dues and subscriptions exceeding 10% of the prior year cost are not approved by the Budget Division of the Department of Finance and Administration.				

Law, Rule, Regulation, etc.	Risk or Exposure	Impact	Likelihood	Control Activity to Ensure Compliance Responsible Area?	Control Operating Effectively?
F&A Policy 11, <i>Recovery of Overpayment to Employees</i>	Overpayments made to employees are not recovered in accordance with the provisions of Policy 11.				
F&A Policy 12, <i>The Use of Journal Vouchers for Billing Those Agencies and Departments Using the Facilities of State Parks</i>	Journal vouchers for the use of state parks are not prepared in accordance with the provisions of Policy 12.				
F&A Policy 13, <i>Receipt Of ACH Debits</i>	Automated Clearing House (ACH) debits are not used according to the provisions of Policy 13.				
F&A Policy 14, <i>Use of Automated Clearing House for Transfer of Funds to Employees and Vendors</i>	Non-payroll payments to employees are not made in accordance with the provisions of Policy 14.				
F&A Policy 15, <i>Assigning Payment Dates for the Processing of Disbursement Vouchers for Payment of Invoices</i>	Payment dates are not accurately recorded in the due date field in STARS.				
	Disbursement vouchers are not submitted to the Division of Accounts at least four (4) business days prior to the due date.				
F&A Policy 16, <i>Employee Housing and Meals</i>	Employee housing plans are not submitted to the Commissioner of Finance and Administration by December 31 of each year.				

Law, Rule, Regulation, etc.	Risk or Exposure	Impact	Likelihood	Control Activity to Ensure Compliance Responsible Area?	Control Operating Effectively?
	Rent is not charged to employees receiving housing in accordance with Policy 16.				
F&A Policy 17, <i>Long Distance Telephone Calls</i>	Personal long-distance calls are made on state telephones.				
	Personal calls are made on state issued cellular telephones.				
F&A Policy 18, <i>Journal Vouchers Type J</i>	Type J journal vouchers are not initiated in accordance with the guidelines established in Policy 18.				
	Journal vouchers received by the paying agencies totaling \$2,500.01 through \$350,000.00 are not processed, completed, entered into STARS and sent to the Division of Accounts or returned with questions to the billing department within (5) working days of the receipt of the journal voucher.				
F&A Policy 19, <i>Issuance of Duplicate Warrants</i>	A duplicate warrant is issued to an employee or vendor without the cancellation of the original warrant.				
F&A Policy 20, <i>Recording of Federal Grant Expenditures and Revenues</i>	All federal grants are not loaded onto the STARS Grant Control Table.				

Law, Rule, Regulation, etc.	Risk or Exposure	Impact	Likelihood	Control Activity to Ensure Compliance Responsible Area?	Control Operating Effectively?
	All grant related expenditure and revenue transactions are not coded with the appropriate grant(s) at the time the initial transaction is recorded.				
	Drawdowns of federal funds are not requested timely.				
	The STARS "Schedule of Grant Activity" Report is not used as the basis for preparing the Schedules of Expenditures of Federal Awards.				
F&A Policy 21, <i>Collateral Deposited with the State</i>	Collateral securities accepted are not in registered form.				
	Collateral securities are received that are not the type of securities the department is authorized to accept under the particular law authorizing or requiring the department to demand the deposit of such collateral.				
	Collateral securities are not fully registered as to principal and interest in such manner as to identify the state and the appropriate agency or department as holder of such collateral and to also identify the individual or concern placing such collateral.				

Law, Rule, Regulation, etc.	Risk or Exposure	Impact	Likelihood	Control Activity to Ensure Compliance Responsible Area?	Control Operating Effectively?
	The State Treasurer is not provided with a listing of individuals authorized to initiate collateral transactions on behalf of the department/agency, and a list of individuals authorized to pick up collateral from the State Treasurer.				
F&A Policy 22, <i>Subrecipient Monitoring</i>	An annual monitoring plan is not submitted to the Department of Finance and Administration, Division of Resource Development and Support, by October 1st of each year.				
	All subrecipients are not identified in the annual monitoring plan.				
	Subrecipients are not monitored in accordance with the requirements of Policy 22.				
F&A Policy 23, <i>Accounts Receivable - Recording, Collection, and Write-Offs</i>	Collection efforts are not made to collect amounts due to the State of Tennessee where goods or services have been provided and payment is due.				
	Accounts receivable are written off without the approval of F&A's Division of Accounts.				

Law, Rule, Regulation, etc.	Risk or Exposure	Impact	Likelihood	Control Activity to Ensure Compliance Responsible Area?	Control Operating Effectively?
F&A Policy 24, <i>Electronic Commerce</i>	Statewide contracts are not used for all forms of electronic commerce including acceptance via use of point-of-sale equipment, telephone, fax, Internet or through charges originating with a third party vendor that is providing services on behalf of the State.				
F&A Policy 25, <i>Deposit Practices Policy</i>	Funds are not deposited immediately as required by TCA 9-4-301 and as defined by F&A Policy 25.				
F&A Policy 26, <i>Employee Fringe Benefits and Supplemental Wages</i>	Fringe benefits and supplemental wages received by State employees are not identified and reported to the Internal Revenue Service.				
F&A Policy 27, <i>Moving Policy</i>	Payment of moving expenses are not approved in advance by the Budget Office of the Department of Finance and Administration.				
F&A Policy 28, <i>Payroll Inserts</i>	Approval for payroll inserts is not obtained in advance from the Chief of Accounts, through the Director of Payroll.				
F&A Policy 29, <i>State Contracts for Credit and Debit Cards</i>	Payment or debit cards are acquired outside the statewide contract established by the Department of Finance and Administration.				

Law, Rule, Regulation, etc.	Risk or Exposure	Impact	Likelihood	Control Activity to Ensure Compliance Responsible Area?	Control Operating Effectively?
	Unauthorized purchases are made with agency credit or debit cards.				
Governor Bredesen Executive Orders # 2 and #3, <i>Conflict of Interest Disclosure Act</i> (T.C.A. §§ 8-50-501 et seq., 2-10-128 and 2-10-129)	The department is not in compliance with the requirements and disclosures required by executive orders #2 and #3.				
<i>Prompt Payment Act</i> (TCA 12-4-703)	Payments are not made on a timely basis and in accordance with all purchase orders and contracts, or within 45 days after receiving the invoice if not specified.				
<i>State Purchasing Manual</i>	Bids are not obtained for purchases when required.				
	Unapproved purchases are made.				
<i>Year-end Accounting Reference Manual</i> promulgated by the Department of Finance and Administration	The Schedule of Expenditures of Federal Awards (SEFA) and Supplementary Information Schedule are not prepared in accordance with the requirements of <i>OMB Circular A-133</i> .				
	The SEFA and Supplementary Schedule are not submitted by the deadline date specified in the <i>Year-end Accounting Reference Manual</i> .				

SECTION VI CONTROL ACTIVITIES

Part 3 Fraud

Instructions

1. Address the following risks and any identified agency-specific risks due to fraud.
2. For each risk, estimate the potential impact to the agency assuming the risk occurs. Use High, Medium or Small.
3. For each risk, assess the likelihood of the risk occurring. Use Probably, Reasonably Possible or Remote. Alternatively, use High, Medium or Low.
4. For each risk with large or moderate impact and probable (high) or reasonably possible (medium) likelihood of occurrence, list the control activity to mitigate the risk to an acceptable level. If no control activity is present to manage the risk, a corrective action plan should be completed and attached. Any N/As should be explained.

Risk Category 1 - Fraudulent Financial Reporting				
Inherent Risk	Impact	Likelihood	Control Activity	Control Operating Effectively?
Use of grant funds for other than specified purpose resulting in revenue not truly having been earned and therefore, overstating revenues.				
Deferring earned revenue to avoid funds reverting to the General Fund.			<i>Example: Deferred revenue accounts are reconciled at year end by independent party.</i>	
Overestimating liabilities to retain residual funding at the end of year.				
Overestimating federal receivables at year end in order to meet reversion target.			<i>Example: Federal receivables are supported with expenditure documentation.</i>	

Inherent Risk	Impact	Likelihood	Control Activity	Control Operating Effectively?
Nondisclosure of pending litigation due to avoidance of public exposure.				
Failure to write down the fair market value of an investment to avoid recording a loss and reflecting poor investment management.				
Delay in the proper accumulation of expenditures of a project to avoid reporting the costs in excess of the amount originally expected or approved to construct an asset.				
Failure to disclose actual risks investments are susceptible to in order to avoid exhibiting management's negligence in ensuring proper collateralization of investments			<i>Example: Accounting personnel are separate from investment function. Investment performance is reviewed quarterly by management.</i>	
Establishing reserves or overstating reserves without proper justification.				
Improper capitalization of expenses, i.e., leases.				
Additional Inherent Risks:	Impact	Likelihood	Additional Control Activity	Control Operating Effectively?

Inherent Risk	Impact	Likelihood	Control Activity	Control Operating Effectively?
Fraud Risk Category 2 - Misappropriation of Assets				
Theft or loss of assets, particularly "sensitive equipment" such as laptops or other computer equipment.				
A requisition for goods or services is defined so narrowly that it appears that only one supplier is available.				
Unapproved removal or disposal of assets e.g. because of alleged damage.			<i>Example: Management approval of all disposal is required.</i>	
Loss of control over assets because asset inventory not maintained.				
Inability to explain and/or itemize expenditure on assets.			<i>Example: Appropriate, complete expenditure classification and explanation on vouchers to facilitate expenditure analysis is required.</i>	
Theft of physical resources such as stationery, tools, etc.				
Inappropriate use of organizational phones, photocopiers, portable and attractive items.				

Inherent Risk	Impact	Likelihood	Control Activity	Control Operating Effectively?
Unauthorized disclosure of personal or confidential information.				
System is manipulated resulting in payments to non existent suppliers.			<i>Example: Personnel with vendor add/change authorization in system is not authorized to perform any payable functions.</i>	
False travel claims submitted.			<i>Example: Travel claims are to be approved by supervisors and supporting documentation is required to support hotel expenses. Mileage is limited to the Official State Map mileage or Rand McNally.</i>	
Theft or "borrowing" of petty cash.			<i>Example: Petty cash is counted and reimbursed by someone independent of the petty cash officer monthly with management's review and signature.</i>	
Submission of bogus petty cash claims.				

Inherent Risk	Impact	Likelihood	Control Activity	Control Operating Effectively?
Receipts not issued for money received.			<i>Example: Cash receipt clerk is segregated from clerk responsible for deposit preparation and accounts receivable. Daily reconciliations are performed between receivables, deposits, cash receipts and cash logs. Customer statements are sent to customers monthly and disputed account balances are not forwarded to cash receipt clerk or to A/R clerk.</i>	
Under-banking or failure to bank cash receipts.			<i>Example: Procedures in place to enable regular reconciliation between documentation, cash receipts, and petty cash claims.</i>	
Theft of cash following permanent closure or relocation of unit.				
Unauthorized access to sensitive data.			<i>Example: Sensitive/confidential information is secured under combination lock. Sensitive information is indicated as such and/or employees are made aware of their fiduciary duties in regards to security of data.</i>	
Use of fuel card for private use.				
An incidence of fraud has been identified, but processes have not been put in place to reduce the risk of repetition.			<i>Example: Incidents of fraud are reported to the internal auditor and audit committee.</i>	

Inherent Risk	Impact	Likelihood	Control Activity	Control Operating Effectively?
Falsification of travel claim mileage.				
False invoices accepted resulting in payment for goods not received.				
Theft of sensitive information from State vehicles.			<i>Example: Managers ensure staff are aware of security of sensitive information. Subject personnel are required to sign "need to know" policy.</i>	
Theft of State owned vehicles from parking areas or while garaged at home.				
Theft or substitution of accessories or tools.				
Payroll payments above approved entitlements.			<i>Example: Salary changes are limited to personnel with granted access. Changes to salaries are printed on computer printout which is signed by management.</i>	
Fictitious employee created by payroll clerk.				

Inherent Risk	Impact	Likelihood	Control Activity	Control Operating Effectively?
Overpayments of employees.				
Fraudulent recording of attendance/time.				
Leave taken and reimbursed for exceeds entitlements.			<i>Example: System does not allow leave taken to exceed leave accrued.</i>	
Staff claiming reimbursement for simultaneous hours in different locations.				
Timesheets altered to increase hours, allowances.				
Conducting personal business during work hours.			<i>Example: Managers ensure staff are aware of policies on issue of departmental resources, including time. All new personnel receives a hard copy of these procedures upon hiring.</i>	
Fraudulent worker's compensation claims.				
Fraud committed through negligence as a result of manager/supervisor not checking claims for payments.				

Inherent Risk	Impact	Likelihood	Control Activity	Control Operating Effectively?
Looting following a natural disaster resulting in loss of data.			<i>Example: Disaster Recovery Plan procedures require immediate security detail on hand as soon as plan is initiated.</i>	
Inadequate application controls resulting in unauthorized staff accessing systems.				
Unauthorized release of user name and/or password.				
Excessive internet browsing.			<i>Example: Personnel are required to sign computer usage policy acknowledgement form.</i>	
Installation of illegal software on State owned computers.				
Downloading of inappropriate material from internet.				
Theft of goods or unauthorized disposal of goods.				
Vendor address is changed in payable system in order to intercept and steal check/warrant.			<i>Example: Vendor information cannot be changed without prior approval of management, supporting documentation and can only be performed by IS personnel who are independent of A/P functions.</i>	

Inherent Risk	Impact	Likelihood	Control Activity	Control Operating Effectively?
Non-substantiated claims for reimbursement.			<i>Example: Original documentation required for support of claims.</i>	
Requests for Proposals integrity compromised as a result of collusion between a contractor and purchase contact.				
Unauthorized personal use of State vehicle.			<i>Example: Supervisors ensure staff understand policy on careful and authorized use of State vehicles.</i>	
Personal items are purchased using agency payment/credit card.				
Employee who is embezzling funds makes a transfer of funds from a bank account (2) in one bank to a bank account (1) where the funds were originally stolen from in another bank near the end of the period. The withdrawal from the second bank account is not recorded and due to timing, does not appear on the year end bank statement and the embezzlement is not detected.			<i>Example: Someone independent of cash disbursement or receipting functions accounts for all check numbers. Also, no checks are made to cash or bearer or a cutoff bank statement is obtained after year end.</i>	

Inherent Risk	Impact	Likelihood	Control Activity	Control Operating Effectively?
Accounts receivable clerk steals customer receipts for account payment and covers with another customer's later payment and so on and at the end of the year, writes off the receivable.			<i>Example: Segregation of duties between cash and accounts receivable records. Also, accounts receivable write offs require prior approval.</i>	
Additional Inherent Risks:	Impact	Likelihood	Additional Control Activity	
Fraud Risk Category 3 - Corruption				
Collusive activity between procurement officer and supplier resulting in invoice higher than approved prices.				
Collusive practices resulting in the purchasing process not being sufficiently competitive.			<i>Example: Staff are required to sign conflict of interest statement. All contracts over a certain dollar amounts are required to have at least three bids.</i>	
Payments for services continue to subrecipients that do not comply with reporting requirements due to collusion.				

Inherent Risk	Impact	Likelihood	Control Activity	Control Operating Effectively?
Services are purchased from an organization/contractor with a previous fraud history or general record of non-compliance with reporting requirement.			<i>Example: Vendors are investigated in system by fed. i.d. number for prior establishment which would determine if prior fraud history existed and vendor was banned in system. Centrally maintained list of banned companies.</i>	
Staff involved in decision making or monitoring may have a personal or pecuniary interest in the contract.				
Unauthorized staff appointments.				
Overtime worked without authorization.			<i>Example: All time entered into system must be approved by management before being released for processing.</i>	
Application for employment using false personal details.				
Appointments made on other than merit.			<i>Example: Original documentation required to be maintained for verification of appointment of staff.</i>	
Kickbacks or spotting fees paid to staff from contractors, suppliers and/or brokers.				

Inherent Risk	Impact	Likelihood	Control Activity	Control Operating Effectively?
Splitting orders to avoid being subject to the bid process.				
Additional Inherent Risks:	Impact	Likelihood	Additional Control Activity	Control Operating Effectively?

SECTION VII

INFORMATION AND COMMUNICATION

Every enterprise and government identifies and captures a wide range of information, relating to external as well as internal events and activities, relevant to managing the entity. Pertinent information is identified, captured, and communicated in a form and timeframe that enable people to carry out their enterprise risk management and other responsibilities. Information systems use internally generated data and information from external sources, providing information for managing risks and making informed decisions relative to objectives. Effective communication also occurs, flowing down, across, and up the organization. All personnel receive a clear message from top management that enterprise risk management responsibilities must be taken seriously. They understand their own role in enterprise risk management, as well as how individual activities relate to the work of others. They must have a means of communicating significant information upstream. Also, effective communication with external parties, such as customers, suppliers, regulators, and shareholders exists.

The following are elements of an effective information and communication system and suggestions for consideration:

Information

Information is needed at all levels of an organization to identify, assess, and respond to risks, and to otherwise run the entity and achieve its objectives. An array of information is used, relevant to one or more objectives categories. Operating information from internal and external sources, both financial and non-financial, is relevant to multiple agency objectives.

- Has an information systems infrastructure been established to source, capture, process, analyze, and report relevant financial and non-financial information?
- Do the information systems incorporate processing of internally generated data as well as external data, for example, market- or industry-specific economic data that signals changes in demand for services, market intelligence on evolving stakeholder preferences or demands, and legislative or regulatory initiatives?
- Do the information systems change as needed to support new objectives in a timeframe and way that are useful in controlling the entity's activities?

Strategic and Integrated Systems

As enterprises have become more collaborative and integrated with customers, suppliers, and business partners, the division between an entity's information systems architecture and that of external parties is increasingly blurred. As a result, data processing and data management often become a shared responsibility of

multiple entities. In such cases, an organization's information systems architecture must be sufficiently flexible and agile to effectively integrate with affiliated external parties.

- While information systems are fundamental to effective enterprise risk management, does management's risk management techniques contemplate organizational goals in making technology selection and implementation decisions?

Integration with Operations

Information systems often are fully integrated into most aspects of operations such as when using web and web-based systems or enterprise-wide information systems (e.g., enterprise resource planning (ERP)). These applications facilitate access to information (i.e., historical and present data) previously trapped in functional or departmental silos, making it available for widespread management use. Transactions are recorded and tracked in real time, enabling managers to immediately access financial and operating information more effectively to control agency activities.

- Does the information system encompass knowledge management capabilities allowing employees to share innovative entity solutions?
- Does the captured historical data allow the entity to track actual performance against targets, plans, and expectations?
- Does management identify correlations and trends from the historical data to forecast future performance that can provide early warning of potential events warranting management attention?
- Does the present or current-state data allow the entity to determine whether it is remaining within established risk tolerances for a process, function, or unit, and to identify variations from expectations?

Depth and Timeliness of Information

The information infrastructure sources and captures data in a timeframe and at a depth consistent with an entity's need to identify, assess, and respond to risk, and remain within its risk tolerances. Timeliness of information flow needs to be consistent with the rate of change in the entity's internal and external environments.

- Does the information infrastructure convert raw data into more meaningful, relevant information to create knowledgeable and wise decisions that assists personnel in carrying out their enterprise risk management and other responsibilities?
- Is information provided in a form and timeframe that are actionable, readily usable, and linked to defined accountabilities?
- To avoid "information overload," has management ensured the flow of the right information, in the right form, at the right level of detail, to the right people, at the right time?

- In developing the knowledge and information infrastructure, has management considered the distinct information requirements of individual users and departments and the summary level information needed by different levels of management.

Information Quality

With increasing dependence on sophisticated information systems and data-driven automated decision systems and processes, data reliability is critical. Inaccurate data can result in unidentified risks or poor assessments and bad management decisions. The quality of information includes ascertaining whether the informational content is appropriate, timely, current, accurate, and accessible.

- Has management established a strategic plan with clear accountability and responsibilities for data integrity?
- Has management performed regular data quality assessments?
- Is the information and data at the right level of detail, there when required, the latest available, correct, and easy to obtain by those who need it?

Communication

Communication is inherent in information systems. Information systems must provide information to appropriate personnel so that they can carry out their strategic, operating, reporting, compliance, and stewardship responsibilities. But communication also must take place in a broader sense, dealing with expectations, responsibilities of individuals and groups, and other important matters.

Internal

Management provides specific and directed communication that addresses behavioral expectations and the responsibilities of personnel. This includes a clear statement of the entity's risk management philosophy and approach and a clear delegation of authority. Communication about processes and procedures should align with, and underpin, the desired culture. Communication should effectively convey the importance and relevance of effective enterprise risk management, the entity's objectives, the entity's risk appetite and risk tolerances, a common risk language, and the roles and responsibilities of personnel in effecting and supporting the components of enterprise risk management.

- Has management required employees to consult with others across the organization as appropriate when new events are identified in order to recognize a problem or determine its cause and corrective action?
- Are all employees clearly aware of what is deemed acceptable and unacceptable behavior?
- Do communication channels ensure personnel can and do communicate risk-based information across agency units, processes, or functional silos, as well

- as upstream to management?
- Are employees encouraged to report suspected violations of an entity's code of conduct without reprisals (i.e., whistleblower protections) for reporting relevant information?
 - Has top management kept the oversight body informed of performance, risk, the functioning of enterprise risk management, and other relevant events or issues?
 - Has the oversight body communicated its information needs to management and provided feedback and direction?
 - Has management communicated entity-wide risks and associated risk responses in regular briefings with all employees?
 - Are enterprise risk management policies, standards, and procedures made readily available to employees along with clear statements requiring compliance?
 - Do new hire orientation sessions include information and literature on the entity's risk management philosophy and enterprise risk management program?
 - Is the risk management philosophy reinforced in regular and ongoing internal communication programs and through specific communication programs to reinforce tenets of the entity's culture?

External

Appropriate communication also needs to exist outside the entity. With open external communications channels, constituents (e.g., citizens) can provide highly significant input on the design or quality of products or services, enabling an entity to address evolving customer demands or preferences. Management should be ready to recognize implications of such circumstances and investigate and take necessary corrective actions, focusing on the impact on financial reporting and compliance as well as operations objectives.

- Has management established an open communication about the entity's risk appetite and risk tolerances?
- Has management considered how its risk appetite and risk tolerances align with those of its business partners, ensuring it does not inadvertently accept too much risk through its partners?
- Are communications to stakeholders, regulators, financial analysts, and other external parties relevant to their needs, meaningful, pertinent, and timely, and in conformance with legal and regulatory requirements?

Means of Communication

The way management deals with personnel can communicate a powerful message. Managers should remember that actions speak louder than words. Their actions are, in turn, influenced by the entity's history and culture, drawing on past observations of how their mentors dealt with similar situations. An entity with a history of

operating with integrity, and whose culture is well understood by people throughout the organization, will likely find little difficulty communicating its message. An entity without such a tradition will need to put more effort into the way messages are communicated. A desirable goal is, over time, to embed communications on enterprise risk management into an entity's broad-based, ongoing communications programs, consistent with the concept of building enterprise risk management into the fabric of the organization.

- Are reporting mechanisms and protocols such that personnel will feel comfortable using the communications channels?
- Do policy and procedure manuals address management's enterprise risk management philosophy?
- Does management conduct regular risk management conference calls among a network of risk champions and other employees?
- Does top management, including the chief risk officer and associated staff, communicate regularly with personnel via email or newsletters from top management?
- Do regular face-to-face meetings occur with "risk champions" or other employees from a range of functions and entity units with responsibility for aspects of enterprise risk management?

SECTION VIII MONITORING

Enterprise risk management is monitored—assessing the presence and functioning of its components over time. Monitoring can be accomplished through ongoing monitoring activities, separate evaluations, or a combination of the two. Ongoing monitoring occurs in the normal course of management activities. The scope and frequency of separate evaluations will depend primarily on an assessment of risks and the effectiveness of ongoing monitoring procedures. Enterprise risk management deficiencies are reported upstream, with serious matters reported to top management and the oversight body.

An entity's enterprise risk management changes over time. Risk responses that were once effective may become irrelevant; control activities may become less effective, or no longer be performed; or entity objectives may change. This can be due to the arrival of new personnel, changes in entity structure or direction, or the introduction of new processes. In the face of such changes, management needs to determine whether the functioning of enterprise risk management continues to be effective.

- Has management considered the nature and degree of changes occurring and their associated risks?
- Has management considered the competence and experience of the personnel implementing risk responses and related controls?
- Has management considered the results of ongoing monitoring?
- Has management built ongoing monitoring into the normal, recurring operating activities of the entity?

Ongoing Monitoring Activities

Many activities serve to monitor the effectiveness of enterprise risk management in the ordinary course of running the entity. These stem from regular management activities, which might involve variance analysis, comparisons of information from disparate sources, and dealing with unexpected occurrences.

- Has management considered the implications of information received such as relationships, inconsistencies, or other relevant implications that raise issues whereby follow up with other personnel is necessary to determine corrective or other actions?
- Has management taken an occasional fresh look at focusing directly on enterprise risk management effectiveness?
- Has management reviewed reports of key entity activity indicators such as key financial and operational statistics?
- Has management reviewed performance against limits established for risk exposures, such as acceptable error rates, items in suspense, reconciling items,

- or credit risk exposure to counterparties?
- Has management reviewed key performance indicators such as trends in direction and magnitude of risks, status of strategic and tactical initiatives, trends or variances in actual results to budget or prior periods, and event triggers, as described in the Event Identification section?

Scope and Frequency

Evaluations of enterprise risk management vary in scope and frequency, depending on the significance of risks and importance of the risk responses and related controls in managing the risks. When a decision is made to undertake a comprehensive evaluation of an entity's enterprise risk management, attention should be directed to addressing its application in strategy setting as well as with respect to significant activities. The evaluation scope also will depend on which objectives categories – strategic, operations, reporting, and compliance – are to be addressed.

- Has management conducted an annual evaluation of the higher-priority risk areas and responses?
- Has management conducted a comprehensive evaluation of the entirety of enterprise risk management at least once every three years or sooner if a major strategy or management change occurs, a program is added or deleted, changes in economic or political conditions exist, or changes in operations or methods of processing information have occurred?

Who Evaluates

Often, evaluations take the form of self-assessments, where persons responsible for a particular unit or function determine the effectiveness of enterprise risk management for their activities. For example, the chief executive of a division directs the evaluation of its enterprise risk management activities. He or she personally assesses the risk management activities associated with strategic choices and high-level objectives as well as the internal environment component, and individuals in charge of the division's various operating activities assess the effectiveness of enterprise risk management components relative to their spheres of responsibility. Line managers focus on operations and compliance objectives, and the divisional controller focuses on reporting objectives. The division's assessments are then considered by senior management, along with evaluations of the company's other divisions.

Internal auditors normally perform evaluations as part of their regular duties, or at the specific request of senior management, the oversight body, or divisional executives. Similarly, management may utilize input from external auditors in considering the effectiveness of enterprise risk management. A combination of efforts may be used in conducting whatever evaluative procedures management deems necessary.

The Evaluation Process

Evaluating enterprise risk management is a process in itself. While approaches or techniques

vary, a discipline should be brought to the process, with certain basics inherent in it.

- Does the evaluator understand each of the entity's activities and each of the components of enterprise risk management being addressed?
- Has the evaluator determined how the enterprise risk management system actually works or functions?
- Has the evaluator held discussions with personnel who perform or are affected by enterprise risk management by examining records on performance or a combination of procedures?
- Has the evaluator analyzed the enterprise risk management process design and the results of tests performed?
- Based on the analysis conducted in accordance with management's established standards for each component, has the evaluator determined whether the process provides reasonable assurance with respect to the stated objectives?

Methodology

A variety of evaluation methodologies and tools are available, including checklists, questionnaires, and flowcharting techniques. As part of their evaluation methodology, some entities compare or benchmark their enterprise risk management process against those of other entities with reputations for having particularly good enterprise risk management. Management could consider the following planning and performance steps in a separate evaluation:

Planning

- Define the objectives and scope of the evaluation
- Identify an executive with requisite authority to manage the evaluation
- Identify the evaluation team, support personnel, and key governmental unit contacts
- Define the evaluation methodology, timeline, and steps to be conducted
- Agree on evaluation plan

Performance

- Gain an understanding of the entity's activities
- Understand how the entity's risk management process is designed to work
- Apply the agreed-on methods to evaluate the risk management process
- Analyze results by comparison to the entity's internal audit standards and follow up as necessary
- Document deficiencies and proposed remediation, if applicable
- Review and validate findings with appropriate personnel

Documentation

The extent of documentation of an entity's enterprise risk management varies with the entity's size, complexity, and similar factors. Larger organizations usually have

written policy manuals, formal organization charts, written job descriptions, operating instructions, information system or process flowcharts, key performance indicators, and so forth. Smaller entities typically have considerably less documentation. Many aspects of enterprise risk management are informal and undocumented, yet are regularly performed and highly effective. These activities may be tested in the same ways as documented activities. The fact that elements of enterprise risk management are not documented does not mean that they are not effective or that they cannot be evaluated. However, an appropriate level of documentation usually makes evaluations more effective and efficient.

- Has the evaluator documented the evaluation process itself?
- Has the evaluator drawn on existing documentation of the entity's enterprise risk management and supplemented this with additional documentation, along with descriptions of the tests and analyses performed in the evaluation?
- When management intends to make a statement to external parties regarding enterprise risk management effectiveness, has management considered developing and retaining documentation to support the statement if the statement subsequently is challenged?
- Does management have a document retention policy?

Reporting Deficiencies

Deficiencies in an entity's enterprise risk management may surface from many sources, including the entity's ongoing monitoring procedures, separate evaluations, and external parties. A deficiency is a condition within enterprise risk management worthy of attention that may represent a perceived, potential, or real shortcoming, or an opportunity to strengthen enterprise risk management to increase the likelihood that the entity's objectives will be achieved.

- Are deficiencies reported to persons directly responsible for achieving business objectives affected by the deficiency?
- Do alternative reporting channels exist for reporting sensitive information such as illegal or improper acts?
- Are specified types of deficiencies reported to more senior management?
- Have protocols been established for what is reported to the oversight body or a specified oversight body committee?
- Is information on corrective actions taken or to be taken communicated back to relevant personnel involved in the reporting process?

Sources of Information

One of the best sources of information on enterprise risk management deficiencies is enterprise risk management itself. Ongoing monitoring activities of an enterprise, including managerial activities and everyday supervision of employees, generate insights from those who are directly involved in the entity's activities. These insights are gained in real time and can provide quick identification of deficiencies. Other

sources of deficiencies are the separate evaluations of enterprise risk management. Evaluations performed by management, internal auditors, or other functions can highlight areas in need of improvement.

- Has management considered from external parties (e.g., customers, vendors and others doing business with the entity, external auditors, and regulators) important information on the functioning of an entity's enterprise risk management?
- Has management taken appropriate corrective actions related to reports from external sources for their implications for enterprise risk management?

What Is Reported

All identified enterprise risk management deficiencies that affect an entity's ability to develop and implement its strategy and to set and achieve its objectives should be reported to those positioned to take necessary action. The nature of matters to be communicated will vary depending on individuals' authority to deal with circumstances that arise and on the oversight activities of superiors.

- In deciding what needs to be communicated, has management considered qualitative factors, as well as quantitative measures, especially when considering the implications of findings related to fraud, waste, and abuse?
- Has management reported particular transactions or events and reevaluated related potentially faulty procedures?
- In addition to deficiencies, has management reported identified opportunities to increase the likelihood that the entity's objectives will be achieved?

To Whom to Report

Information generated in the course of operating activities usually is reported through normal channels to immediate superiors. They in turn may communicate upstream or laterally in the organization, so that the information ends up with personnel who can and should act on it. Alternative communications channels also should exist for reporting sensitive information such as illegal or improper acts.

- Are findings of enterprise risk management deficiencies reported to the individual responsible for the function or activity involved, as well as to at least one level of management above that person?
- Where findings cut across organizational boundaries, does the reporting cross over as well, and is it directed to a sufficiently high level to ensure appropriate action?

Reporting Directives

Providing needed information on enterprise risk management deficiencies to the right party is critical. Protocols should be established to identify what information is

needed at a particular level for effective decision making.

- Has a manager received information that affects actions or behavior of personnel within his or her responsibility, as well as information needed to achieve specific objectives?
- Has the commissioner been apprised of serious infractions of policies and procedures?
- Has the commissioner requested and received supporting information on matters that could have significant financial impacts or strategic implications or that could affect the entity's reputation?
- Have senior managers been apprised of risk management and control deficiencies affecting their units (e.g., circumstances where assets with a specified monetary value are not adequately protected, where the competence of employees is lacking, or where important financial reconciliations are not performed correctly)?
- Have specific directives been established regarding what should be reported (e.g., only those deficiencies meeting a specified threshold of seriousness or importance) to the audit committee, board of directors, or other oversight body?

Management Report—Annual Assessment
(Illustrative Sample)

Date _____

The Honorable _____, Commissioner

Department of Finance and Administration
State Capitol
Nashville, TN 37243

And

The Honorable _____

Comptroller of the Treasury
State Capitol
Nashville, TN 37243

Re: Tennessee Financial Integrity Act Guidelines

Dear Sir and/or Madam:

This annual report addresses the agency-wide risk management and internal control requirements of the TCA §9-8-101, known as the *Tennessee Financial Integrity Act*, as amended. In order to assess the effectiveness of our internal control system and of individually significant controls, we conducted an evaluation in accordance with the guidance set forth under TCA §9-18-103. We understand that this guidance was developed using the established comprehensive internal control frameworks entitled *Internal Control—Integrated Framework (1994)* and *Enterprise Risk Management—Integrated Framework (2004)*, issued by the Committee of Sponsoring Organizations (COSO) of the Treadway Commission and published by the American Institute of Certified Public Accountants, and have referred to these frameworks as necessary throughout the evaluation.

The objectives of the Department of _____'s annual risk management and internal controls assessment are to provide reasonable assurance of the following:

- accountability for meeting program objectives;
- promoting operational efficiency and effectiveness;
- improving reliability of financial statements;
- strengthening compliance with laws, regulations, rules, and contracts and grant agreements; and

- reducing the risk of financial or other asset losses due to fraud, waste, and abuse. Funds, property, and other assets are safeguarded against waste, loss, unauthorized use, or misappropriation.

The concept of reasonable assurance recognizes that the costs of internal controls should not exceed the benefits derived from those controls. Reasonable assurance is a high but not an absolute level of assurance. In the course of any review, estimates and judgments are required to assess the expected benefits and related costs of control policies and procedures. Errors or fraud may occur and not be detected due to inherent limitations in any system of risk management and internal control, including those limitations resulting from resource constraints, legislative restrictions, and other factors. Risk assessment allows the agency to consider the extent to which potential events have an impact on achievement of objectives and to mitigate the risk of events that could have a negative impact.

As head of this Department/Agency, we have performed an entity-wide risk assessment and have fully complied with the requirements specified in TCA 9-18-102. To reduce the effect of unacceptable risks, a system of internal control has been implemented and tested for operating effectiveness. I acknowledge responsibility for establishing, implementing, and maintaining an adequate internal control system to prevent and detect fraud, waste, and abuse and for performing this assessment of the operating effectiveness of the department's risk management and internal controls. The results of this assessment have given me reasonable assurance that the Department's/Agency's (*choose appropriate title*) internal controls in effect on a June 30 fiscal year ending basis, adequately safeguard assets, and when taken as a whole provide reasonable assurance of the proper recording of financial transactions; compliance with applicable laws, regulations, rules, contracts and grant agreements; and the achievement of operational objectives, subject to the limitations described in the previous paragraph. As head of this agency, I acknowledge responsibility for maintaining the internal control system of this agency/department.

The attached documents reflect the results of our agency-wide risk assessment and the controls that are intended to mitigate the identified risks.

Sincerely

Commissioner (or Agency Head)
(signature)

Report Checklist

STAGE 1—INITIAL ASSESSMENT

Step 1—Internal Environment

These steps are to be performed to give management a big picture of or to “get-to-know” their organization in order to direct them to their agency’s risks, strategies and objectives.

Has management addressed the following elements of the Internal Environment?

- Risk Management Philosophy
- Risk Appetite
- Integrity and Ethical Values
- Commitment to Competence
- Organizational Structure
- Assignment of Authority and Responsibility
- Human Resource Standards

Step 2— Objective Setting

The goal in step 2 is to identify (1) why the agency exists, (2) what needs to be done and (3) what activities are necessary to achieve its objectives.

Has management addressed the following categories of objectives with respect to its agency?

Strategic Operational Reporting Compliance

Has management identified the business processes and activities its agency participates in to meet its objective?

STAGE 2—RISK ASSESSMENT

Step 3—Event Identification

In Step 3, the goal is to first identify events and then the risks that are produced as a result of those events that would impede the agency in meeting its objectives/performing the activities that are performed to meet those objectives.

- Has management identified events that would impede in the agency meeting its objectives
- Has management listed risks generated from those events?

_____ **Step 4—Likelihood/Impact**

The goal here is to assess and document management's assessment on the likelihood and impact of a risk.

- For each risk identified in Step 3 and those identified in the worksheet template in Section VI

_____ **Step 5—Control Activities and Risk Response**

In Step 5, the agency will identify its control activities. This is where the internal control evaluation takes place. These control activities are to serve as risk responses as well as to ensure that risk responses are carried out.

- For all risks that are high or medium impact and probable or reasonably possibly to occur, has the agency addressed control activities/actions to mitigate those risks?
- Has management tested controls for operating effectiveness?

_____ **Step 6—Final Evaluation**

- Has the agency evaluated its residual risks in the aggregate to determine if total residual risks are within the agency's risk appetite?

STAGE 3—REPORTING

_____ **Step 7—Reporting Package**

- Has management completed the Management Report?
- Has management included this checklist with the report?
- Has management included documentation of their agency-wide risk assessment and internal control evaluation?

BIBLIOGRAPHY

Tennessee's Governmental Accountability Act of 2002, Tennessee Code Annotated, Section 9-4-56

The Financial Integrity Act, Tennessee Code Annotated, Section 9-18-102

Committee of Sponsoring Organizations of the Treadway Commission (COSO), *Enterprise Risk Management—Integrated Framework, 2004*; Website: CPA2biz.com

Committee of Sponsoring Organizations of the Treadway Commission (COSO), *Internal Control—Integrated Framework, 1994*; Website: CPA2biz.com

Statement on Auditing Standards No. 55, *Consideration of Internal Control in a Financial Statement Audit*, Website: CPA2biz.com

Statement on Auditing Standards No 78, *Consideration of Internal Control in a Financial Statement Audit, an Amendment to Statement on Auditing Standards No. 55*, Website: CPA2biz.com

Statement on Auditing Standards No 94, *The Effect of Information Technology on the Auditor's Consideration of Internal Control in a Financial Statement Audit*, Website: CPA2biz.com

Statement on Auditing Standards No. 99, *Consideration of Fraud in a Financial Statement Audit*, Website: CPA2biz.com

Statement on Auditing Standards No.112, *Communicating Internal Control Related Matters Identified in an Audit*, Website: CPA2biz.com

Government Auditing Standards issued by the Comptroller General of the United States, Website: GAO.gov

Statements of the Governmental Accounting Standards Board, Website: GASB.org