TN Department of Finance & Administration

**Management's Guide for Enterprise Risk Management and Internal Control**

**Purpose and authority:** This document provides the implementing guidance for the Financial Integrity Act of 1983 (TCA 9-18-101). It is intended to assist state managers in improving the accountability and effectiveness of state programs, as well as support operations, through the implementation of enterprise risk management practices and by establishing, maintaining and assessing internal control effectiveness. The guide emphasizes the need to integrate and coordinate risk management and effective internal control into existing business activities and as an integral part of managing a state agency or institution of higher education (both herein after referred to as agency).

**Introduction:** Simply put, risk management and internal control should be considered as a means to achieving an end, i.e. making sound decisions to achieve agency objectives without surprises. They can be viewed as two sides of the same coin in that risk management focuses on the identification of threats and opportunities, and controls are designed to effectively counter threats and take advantage of opportunities.

As complementary, not competitive, frameworks, risk management and internal control systems are an integral part of enterprise risk management (ERM). ERM goes beyond periodic risk and process-level control identification by managing the uncertainties that could influence the achievement of an agency's objectives.

ERM aims to enhance, not replace, an agency's normal management processes by providing a comprehensive view and consistent analysis of risks and opportunities to inform management decisions. It is meant to be integrated with management processes such as strategic planning and budgeting.

In summary, ERM modernizes internal control efforts by integrating risk management and internal control activities into an ERM framework to improve mission delivery, reduce costs, and focus corrective actions towards key risks. Essentially, ERM sets the strategy for an agency while internal control is the execution of that strategy.

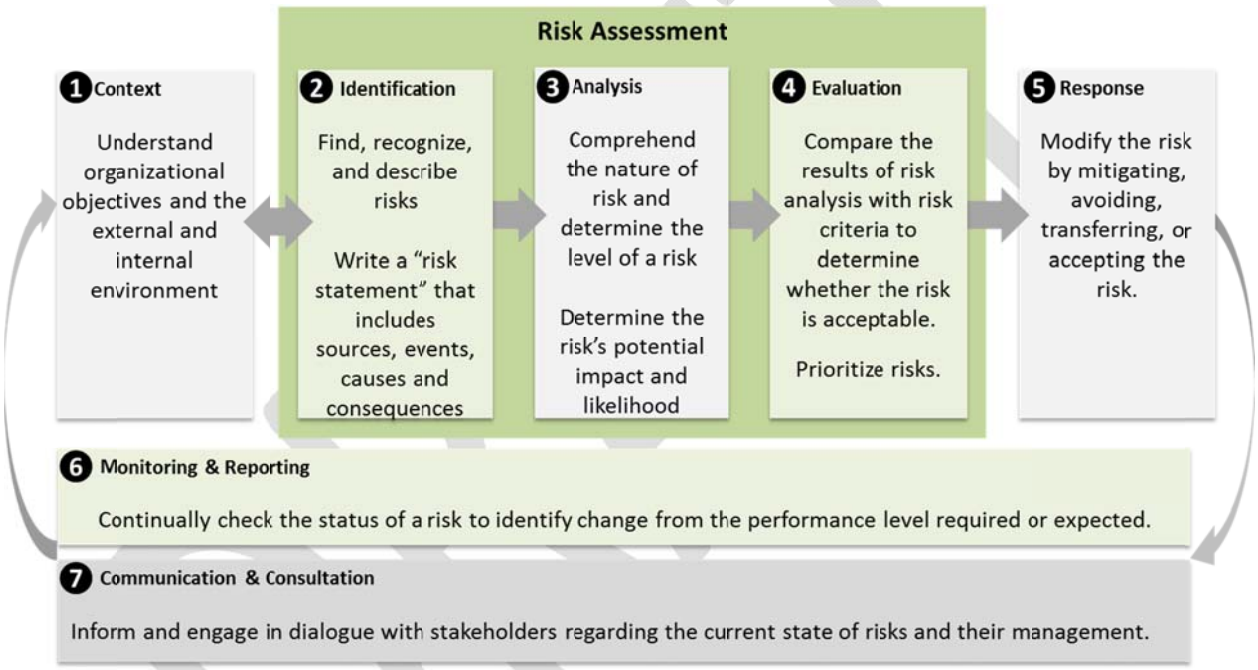
**Overview of an Enterprise Risk Management Process**

The risk management process of identifying, analyzing, evaluating, and ultimately responding to and monitoring risk is at the heart of ERM. Extending this process across an entire agency, looking at both

DRAFT

upside and downside risk, and considering risk in the context of strategy is what differentiates ERM from traditional risk management.

The context (internal and external environment) and the risk assessment steps (identification, analysis, and evaluation) should form the basis for decision-making about which risks or opportunities are priorities, what the appropriate response should be, and how resources should be allocated to manage the risk or opportunity in a way that best supports an agency's strategy. The risk response step involves deciding on and planning for the best way to treat or modify the risk, and implementing that plan. Monitoring and reporting on the status of risks and their management and communication and consultation with stakeholders take place throughout the risk management process.




The end results of the process should enhance agency decision-making by providing senior management with timely and robust information that improves their understanding of enterprise-level risks and opportunities, but any individual at any level in an agency should be able to use portions of the results of the process to assess and plan responses to risks and opportunities in their area.

**Risk Assessment Requirements**

*State agencies and institutions of higher education are required to integrate risk management and internal control functions through formal and informal channels into the elements of the agency's system*

*of management in which they are intended to operate, including the related objectives, activities, processes, systems, risks and responsibilities.*

State leaders and managers are responsible for establishing and achieving goals and objectives, seizing opportunities to improve effectiveness and efficiency of operations, providing reliable reporting, and maintaining compliance with relevant laws and regulations. They are also responsible for implementing management practices that effectively identify, assess, respond, and report on risks.

These responsibilities are carried out through a governance structure defined through a variety of sources, including laws and numerous directives and policies. ERM and internal control should be components of this governance system. ERM as a discipline deals with identifying, assessing, and managing risks. Through adequate risk management, agencies can concentrate efforts towards key points of failure and reduce or eliminate the potential for disruptive events. Internal control is a process effected by an entity's oversight body, management, and other personnel that provides reasonable assurance that the objectives of an entity relating to operations, reporting and compliance will be achieved. Effective internal control is therefore an integral part of an organization's governance system and ability to manage risk.

The Relationship Between Internal Controls and Enterprise Risk Management, OMB Circular No. A-123, Management's Responsibility for Enterprise Risk Management and Internal Control

*There are several ERM models available to help state agencies and institutions of higher education integrate risk management and internal control activities into a common framework. Each agency and institution of higher education should determine what tools and techniques work best in its unique context. (ERM should be considered an iterative process. As ERM capabilities mature, so should the model(s) and tools utilized.)*

*Whatever the model and tools utilized, they must be in alignment with COSO's enterprise risk management framework, and, incorporate the Standards for Internal Control in the Federal*

*Government's (known as the Green Book) adaption of COSO's Internal Control – Integrated Framework (2013).*[1]

**Fundamental Concepts and Compliance Requirements**

Risk should always be assessed in light of setting and achieving an agency's objectives. Linking risks with objectives will help ensure that the risk identification process focuses on those risks that matter, rather than being distracted and diverted by irrelevant risks and uncertainties.

The selected ERM methodology should provide a comprehensive view of risk in terms of the agency's mission and objectives. (Agencies were not created to just do accounting, but to execute missions and important programs benefiting the citizens of Tennessee.) An enterprise-wide, strategically-aligned portfolio view of organizational challenges (e.g. reputational, programmatic performance, financial, information technology, human capital) provides insight about how to most effectively prioritize resource allocations to ensure successful mission delivery.

While agencies cannot respond to all risks related to achieving strategic objectives and performance goals, they must identify, measure, and assess risks related to mission delivery.

Risk management practices should be forward-looking and designed to help leaders make better decisions, alleviate threats and to identify previously unknown opportunities.

The responsibilities of managing risks should be shared throughout the agency from the highest levels of executive leadership to the service delivery staff executing state programs.

A process for considering risk appetite and tolerance levels should be included. The concept of risk appetite is key to achieving effective ERM, and is essential to consider in determining risk responses. Although a formally documented risk appetite statement is not required, agencies must have a solid understanding of their risk appetite and tolerance levels in order to create a comprehensive enterprise-level risk profile. Risk appetite can be considered qualitatively and/or quantitatively and should be factored into the process of balancing risks with opportunities. Additionally, risk appetite and tolerance levels should be evaluated on a regular basis and adjusted accordingly to meet the needs of the organization.

A risk profile should be maintained. The primary purpose of a risk profile is to provide a thoughtful analysis of the risks an agency faces toward achieving its strategic objectives arising from its activities and operations, and to identify appropriate options for addressing significant risks. The risk profile assists in facilitating a determination around the aggregate level and types of risk that the agency and its management are willing to assume to achieve its strategic objectives. The risk profile differs from a risk

[1] http://www.coso.org/
http://www.gao.gov/greenbook/overview

DRAFT

register in that it is a prioritized inventory of the most significant risks identified and assessed through the risk assessment process versus a complete inventory of risks.

Agencies have discretion in terms of the appropriate content and format for their risk profiles; however, in general risk profiles include the following components:

1. Identification of objectives (strategic, operations, reporting and compliance)
2. Identification of risk (initial and continuous)
3. Inherent risk assessment (exposure arising from a specific risk before any action has been taken to manage it beyond normal operations)
4. Current risk response (action taken to manage the risk, i.e. acceptance, avoidance, reduction or sharing)
5. Residual risk assessment (exposure remaining from inherent risk after action has been taken to manage it)

*Note: By their nature, agency risk profiles include information related to internal vulnerabilities. As such they will often contain confidential or sensitive information. Agencies should consult with their Office of General Counsel if there are questions regarding the disclosure of such information.*

Internal control should be made an integral part of the entire cycle of strategic planning, goal and objective setting, budgeting, program management, accounting and auditing. It must support the effectiveness and the integrity of every step of the process and provide continual feedback to management.

Effective internal control should be developed and maintained consistent with established risk appetite and risk tolerance, and integrated into operations in a risk-based and cost beneficial manner, in order to provide reasonable assurance that the agency's internal control over operations, reporting and compliance is operating effectively.

An agency's risk profile should include an evaluation of fraud risks and use a risk-based approach to design and implement financial and administrative control activities to mitigate identified material fraud risks.

The management of risk should be regularly reviewed to monitor whether or not the risk profile has changed and to gain assurance that risk management is effective or if further action is necessary. In addition, processes must be put in place to review whether risks still exist, whether new risks have arisen, whether the likelihood and impact of risks have changed, to report significant changes that adjust risk priorities, and deliver assurance on the effectiveness of internal control. In addition, the overall risk management process must be subjected to regular review to deliver assurance that it remains appropriate and effective.

Correcting control deficiencies is an integral part of management accountability and should be considered a priority by the agency.

DRAFT

**Documentation**

State agencies and institutions of higher education must maintain adequate written documentation of their ERM activities. Dependent upon an agency's scale of operations, as well as the ERM framework/model (or hybrid) selected for use, this documentation may be fairly simple, or necessitate the development of databases or specific tools to assist with the process.

At a minimum the documentation should contain a statement of awareness and compliance with these TCA 9-18-102 guidelines, as well as COSO's ERM components, and, be sufficient to meet the documentation requirements detailed in OV4.08 of the Green Book.

*Word of caution: Many quality internal control questionnaires and checklists are available on the internet. These internal control questionnaires and checklists list common risks and control activities for various processes. However, because these questionnaires and checklists were authored by experts unfamiliar with Tennessee agency's operations, they are unlikely to be sufficient for documenting your organization's risk assessment process. Nevertheless, these questionnaires and checklists may be useful in validating the completeness of a risk assessment once it has been prepared and provide users with common control activities.*

**Responsibility**

Each agency's responsibility for assessing risk and implementing internal control standards begins with the chief executive officer (agency head) and extends to everyone in the agency. In practice, the agency head will delegate the operation of the risk management framework to the senior management team, who will be responsible for completing the necessary activities. There may be a separate function that co-ordinates and manages these activities and brings to bear specialist skills and knowledge.

Internal auditors can have vital roles in the ERM function. In many agencies the internal auditor is best positioned to fully understand the scope of an agency's strategies and related strategic risks. More informed risk taking and decision making can result from using the strengths and competencies of the internal audit function through its participation in the implementation and execution of an ERM program. The internal auditor should not, however, be responsible for managing risks or making decisions on behalf of management.

**Annual Reporting**

The head of each state agency and higher education institution is required to file an annual assurances report with the commissioner of finance and administration and the comptroller of the treasury on or before December 31. As outlined in TCA 9-8-104, the assurances report must include executive

DRAFT

management's acknowledgement of its responsibility for establishing, maintaining and assessing internal control effectiveness; and, include a statement of assurance representing the agency head's informed judgement as to the overall adequacy and effectiveness of internal controls related to program objectives; operational efficiency and effectiveness; financial reporting; compliance with laws, regulations, rules, contracts and grant agreements; and, fraud, waste and abuse. This statement must take one of the following forms:

Unmodified statement of assurance (no material weakness or lack of compliance reported), or

Modified statement of assurance, considering the exceptions explicitly noted (a corrective action plan must accompany any modified statement).

The results of the agency's risk assessment processes should support and provide the basis for the provided assurance.

The agency head must sign the assurances report.

## Bibliography

*Portions of this guide summarized from one or more of the following sources:*


Association of Government Accountants (AGA). "2016 ERM and Internal Controls Forum Summary." *Executive Report*. 2016.

Committee of Sponsoring Organizations of the Treadway Commission (COSO). "Enterprise Risk Management-Integrated Framework." 2004.

Commonwealth of Massachusetts, Office of the Comptroller. "Revised-Commonwealth Internal Control Guide." 25 June 2015.

J. Stephen McNally, CPA, and Vincent H. Tophoff, RA. "Leveraging Effective Risk Management and Internal Control." *Strategic Finance* April 2014.

Minnesota Management & Budget . "Guide to Risk Assessment and Control Activities." May 2012.

Protiviti Inc., Independent Risk Consulting. "Guide to Enterprise Risk Management, Frequently Asked Questions." January 2006.

Tennessee Comptroller of the Treasury. "Internal Control and Compliance Manual for Governmental Entities and Other Audited Entities in Tennessee." December 2015.

United Kingdom, HM Treasury. "The Orange Book, Management of Risk - Principles and Concepts ." October 2004.


DRAFT

United States Government Accountability Office, by the Comproller of the United States. "Standards for Internal Control in the Federal Government (Green Book)." September 2014.

United States Office of Management and Budget (OMB). "OMB Circular No A-123, Management's Responsibility for Enterprise Risk Management and Internal Control." 15 July 2016.

University of Vermont. "Guide to Risk Assessment & Repsonse." *Enterprise Risk Management Program*. 16 August 2012.

Washington State, Office of Financial Management. "Chapter 20, Internal Controls and Auditing (20.15 Internal Control Basics and 20.20 Risk Assessment)." *State Administrative & Accounting Manual (SAAM)*. July 2008.

DRAFT