MIDDLE TENNESEE STATE UNIVERSITY RISK MANAGEMENT MANUAL

Office of Compliance and Enterprise Risk Management

This Risk Management Manual outlines the risk framework and resources utilized for institution-wide risk management controls and response planning for Middle Tennessee State University.

By: Gené Stephens, J.D., LL.M.
Assistant Vice President – Office of Compliance and Enterprise Risk Management
Division of Business and Finance
gene.stephens@mtsu.edu

I AM trueBLUE.
MIDDLE TENNESSEE STATE UNIVERSITY

Table of Contents

I. Acknowledgements and Introduction

The structure, impact, and success of risk management programming and corporate compliance activities depends largely on an institution's commitment and understanding of risk in relation to its mission and goals. The commitment to risk management and compliance planning also must begin at the senior management level in support of risk programming oversight to ensure participation and engagement in every segment of the campus community, from the Board of Trustees to the Faculty and staff.

Middle Tennessee State University (MTSU, University, or Institution) is a leader in student success performance, academic instruction, and strong operational management that supports both scholarly innovation and sustainable business processes for the continued advancement of the Institution's mission and strategic vision. The University is committed to risk management planning through annual risk assessment activities of each institutional division, including the President's Office. In addition, MTSU demonstrates its commitment to risk assessment planning through continuously improving the effectiveness and efficiency of its operations and policies. The University's risk assessment framework and philosophy also ensures the Institution's compliance with federal, state, and local regulations, as well as the achievement of its strategic objectives.

The author of this Middle Tennessee State University Enterprise Risk Management Manual (Manual) acknowledges the leadership, support, and guidance of the University President; Vice President for Business and Finance; Office of University Counsel; MTSU Board of Trustees; Chief Audit Executive; Director of Financial Compliance; and the collaboration and cooperation of campus Vice Presidents, management, Faculty, and Staff who regularly contributed to, and participated in, the Institution's enterprise-wide compliance and risk assessment activities.

For additional information regarding the risk management activities of Middle Tennessee State University, please contact the Assistant Vice President for Compliance and Enterprise Risk Management in the Division of Business and Finance at the Cope Administration Building, Room 119, at extension 8812.

II. Risk Management Framework

Risk management is utilized in every segment of business and government operations. The risk management framework is an integrated process of both safeguards and strategies to minimize risk exposure. The Committee on Sponsoring Organizations of the Treadway Commission (COSO) provides a risk framework comprised of key components, principles, and concepts to guide enterprise risk management activities for organizations.

There are eight COSO components of enterprise risk management, which are integrated and aligned with the five components of an organization's internal control framework. The components are as follows:

- **Internal Environment** – This COSO component sets the tone of the organization and establishes the basis for how risk is viewed and addressed. The Internal Environment also establishes the organization's risk management philosophy and tolerance, which are interwoven into the ethical values of the operational environment.

- **Objective Setting** – The COSO framework requires organization's to begin the work of managing risk by establishing objectives that align with the mission and goals of the organization. Objectives also should be consistent with the organization's risk tolerance.

- **Event Identification** – Events (both internal and external) affecting the achievement of an organization's objectives that must be identified and distinguished between risks and opportunities.

- **Risk Assessment** – The analyzation of risk, considering the likelihood and impact of risk as a basis for determining how the risk should be managed. Risks are categorized as inherent and residual.

- **Risk Response** – Management's response to risk; namely: avoiding, accepting, reducing, transferring, or sharing risk. The risk response is also developed aligned with an organization's risk appetite or risk tolerance.

- **Control Activities** – Policies and procedures that are implemented to ensure risk responses are executed.

- **Information and Communication** – Relevant information that is disseminated to help an organization carry out its responsibilities. More effective streams of communication flows from the top down, across, and up.

- **Monitoring** – The ongoing process of evaluations and management activities to review an organization's risk management for effectiveness while making modifications, as necessary.

An additional component of enterprise risk management, which is not mentioned within the COSO framework, but aligned with COSO's internal control principles, is the component of reassessment. After an organization has identified risks, assessed risks, responded to risks, implemented control activities, communicated, and begun monitoring and evaluating risk, the risk assessment process must begin again. Such reassessment practices help to measure risk control trends and the effectiveness of such control activities over time.

II.1 Internal Control Framework and Business Objectives

Linked to the risk management framework are the five interrelated components of an organization's internal control. Similar to the risk assessment framework, the COSO internal control framework for organizations encompasses the following components:

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

The components of each framework (risk management and internal control) are further divided into four business categories and objectives:

- Strategic – high-level goals that support organizational mission.
- Operations – effective and efficient use of business resources.
- Reporting – reliability of reporting and data.
- Compliance – compliance with federal, state, and local laws and regulations, as well as regional and programmatic accreditors.

II.2 Board of Trustees Oversight

The role of the Board of Trustees (Board) in the University's enterprise risk management program (Program) is to provide guidance regarding the Program's effectiveness, as well as strategic oversight of the Program's risk controls. Specifically, through its Audit and Compliance Committee, the Board will:

- Review and approve the policy regarding the enterprise risk management program.

- Review and approve the University's State reporting submissions.
- Provide guidance regarding the effectiveness of risk management processes.
- Recommend actions or policies to improve the enterprise risk management program.

II.3 President's Review

The University President will provide initial review and approval, as appropriate, of the enterprise risk management program. The President also will be provided annual reporting on the major risks facing the University. In collaboration, with the Board, the President will provide guidance regarding risk management policies, corporate compliance activities, and actions or policies of the risk management program that will further enhance the University's mission and strategic goals.

II.4 Vice President Review

The institution's Vice Presidents are responsible for the risk management reporting activities within their division, which includes:

- Identifying risks in their Divisional area.
- Developing and implementing risk controls for their Divisional area.
- Providing risk assessment reporting information on designated, State of Tennessee forms in a timely manner for submission to the Director of Financial Compliance.
- Ensuring the existence of performance standards for the implementation of Divisional risk controls and procedures.

II.5 Role of Directors, Managers, Faculty, and Staff

The role of the Directors, Managers, Chairs, Deans, Faculty, and staff regarding risk management programming is to incorporate risk management into their standard practices by:

- Reporting significant or emerging risks in their areas.
- Reviewing the suite of corporate compliance related training presentations provided by the Office of Compliance and Enterprise Risk Management and making department members aware of its resources.
- Developing a register of department risks and risk controls or mitigation methods.

II.6 Role of Audit and Consulting Services

Audit and Consulting Services provides financial auditing and management consulting to the University's campus departments with financial reporting to the MTSU President and the Audit and Compliance Committee. Audit and Consulting Services also collaborates with the Office of Compliance and Enterprise Risk Management regarding risk assessment reporting activities and risk management program effectiveness.

III. Regulatory Compliance Matrix

The MTSU Regulatory Compliance Matrix (Compliance Matrix) provides a guide of federal regulations and laws applicable to the University's operations, student support services, academic offerings, and financial aid. The Compliance Matrix can be found on the Office of Compliance and Risk Management's website.

IV. Risk Assessment Process

The Risk Assessment process involves steps and actions that reduce the likelihood, and significance of risk occurring. As part of its risk management process, the University follows a systematic three-year risk review of its divisions and departments, including the President's Office. In addition, the MTSU risk assessment process aligns with both the Tennessee State Department of Finance and Administration's Risk Management program and COSO Principles. The institution currently utilizes the State's Risk Management Toolset of Forms to appropriately map the University's internal risk environment, objectives, and controls. The following are areas of the Risk Assessment process.

IV.1 Identification

Enterprise-wide risk assessment begins with unified planning and achievable objectives. After the planning and objective stage of the risk assessment process, risk identification is the next step. Risk identification includes both major risks, residual risks, and risk factors (internal and external). Major risks include the loss of operations, financial aid, student services, or the destruction or damage of physical assets. Residual risks are those risks that remain after the implementation of controls. Risk factors, whether internal or external, assists in determining risk severity and risk ranking in terms of severity levels. Examples of risk factors include State or government financial appropriations and funding; new or changing legislation; enrollment changes; or changes in key, institutional personnel.

IV.2 Analysis

After risks have been identified, analysis is necessary to: (1) prioritize the risks (from high-level to low-level); (2) review the risks to determine if there are current controls in existence that failed; (3) determine if new controls are needed; (4) estimate the significance of the risk relative to its financial, reputational, or programmatic loss to the University; and (5) determine the likelihood of occurrence or reoccurrence of the risk. Existing risks, or risk that have been previously identified, may have decreased due to mitigation, controls, monitoring, or a combination of the aforementioned.

IV.3 Controls

Practices, processes, and policies that provide assurances of avoidance or substantial mitigation of an adverse event or action are the purpose of risk controls and control systems. Data and data validation (analysis), as well as information regarding the business operations, internal strategy to move the business forward, and the external climate and competitor factors, are all tools that assist in developing a work plan or system of controls to address risks based on risk priority. Risk controls must also align with the organization's risk tolerance.

IV.4 Monitoring

A key element of the risk management work plan (which contains risk controls for risk reduction, avoidance, or acceptance) is a plan and method for regular monitoring to determine: (1) the effectiveness of controls in reducing or mitigating risk; (2) the awareness of risk controls and institutional processes, practices, and procedures by Faculty, staff, administrators, and Executives; and (3) whether the current controls are keeping up with the institution's business model.

IV.5 Reassessment

After completing all areas of the risk assessment process, the process must begin again as part of the process of continuous improvement, as well as to remain current with organizational, industry, and regulatory changes.

IV.6 Risk Questionnaire

The following is a list of common questions provided in a Risk Assessment Questionnaire to assist departments with risk management activities:

1. What is the mission of the Division/Department/unit?

    a. What are its objectives and goals?

2. How does your department contribute to the University's:
    a. Access?
    b. Quality?
    c. Resourcefulness?
    d. Student Success?

3. For each objective or goal, identify events or issues that might interfere with or prevent the attainment of objectives and goals. What might cause current objectives and goals to shift to new or revised objectives and goals?

    a. **List external and internal factors**. External factors include – changes in regulations or legislation, and reductions in State financial outlays. Internal factors include – departures of key staff members, and budget changes.

    b. **Businesses processes and procedures.** As business models change (e.g. governance, strategy, or increases/decreases in enrollment), so too will the policies, processes, and procedures change that support the model.

    c. **Staff training.** Training that is current and interactive can positively contribute to the attainment of an organization's objectives or goals.

    d. **Contingency planning.** Contingency planning may be necessary if, after assessment and monitoring of risk, controls fail to yield the desired results or in the event of a major disruption of services or assets. Contingency planning also may require adjustments to risk responses (proactive controls versus reactive controls) or adjustments to the institution's risk and compliance program.

4. What risks have increased or decreased in the last year?

5. Have we been successful at risk management, and how do we measure success?

V. MTSU Areas of Risk Assessment

There are seven (7) major processes and areas for which the University performs risk assessments. The areas include:

- Information Technology
- President’s Office
- University Provost
- Financial Management (Business and Finance)
- Student Services
- University Advancement
- Marketing and Communications

In addition to the above areas, the following areas are reviewed for compliance with regulations and risk controls:

- ADA Accessibility
- Equity and Compliance (Title IX)
- Clery Compliance
- Export Control (Research)
- Intellectual Property
- Minors on Campus (Summer Camps)

VI. Enterprise Compliance and Risk Management Committee

VI.1 Charge

The MTSU Enterprise Compliance and Risk Management Committee (ECRMC or Committee) will promote the University's community standards of honesty and integrity, while fostering a culture of ethics, accountability, and risk identification and mitigation. The ECRMC also will work to support the progress and continued success of MTSU by contributing to the design and implementation of an enterprise Compliance Plan that: (1) assists the University in preventing fraud, waste, and abuse of institutional assets; (2) considers innovative solutions to workplace risks, risk controls, and risk management; and (3) encourages organizational participation in enterprise compliance activities. Finally, the Committee will serve as an additional support and resource to the MTSU community regarding regulatory reporting and risk management best practices consistent with the requirements of the State of Tennessee's Division of Finance and Administration. The ECRMC's establishment is recommended pursuant to the United States Sentencing Commission's Guidelines for organizations regarding the seven (7) elements of an effective corporate compliance program (U.S. Sentencing Comm'n Guidelines § 8B2.1).

VI.2 Composition

The Enterprise Compliance and Risk Management Committee should be composed of:

- ❖ two faculty representatives, one of whom should be a member of the graduate faculty;
- ❖ one attorney representative from the Office of University Counsel;
- ❖ one administrator representative from the Office of Research Services;
- ❖ one administrator representative from Student Services;
- ❖ one administrator representative from the Office of Institutional Equity and Compliance;
- ❖ one administrator representative from both Academic Affairs and International Student Affairs;
- ❖ one administrator representative from Human Resources;
- ❖ one administrator representative of Technology Services;
- ❖ one representative from Athletics;
- ❖ one administrator representative from both Facilities and Campus Planning;
- ❖ one administrator representative of Business and Finance;
- ❖ one officer or administrator representative from the University Police; and
- ❖ one representative from the Office of Audit and Consulting Services.

The chair of the ECRMC shall be the Assistant Vice-President for Compliance and Enterprise Risk Management. The Committee shall maintain meeting minutes and other documentation, as necessary. The Committee shall meet twice annually. A schedule of meeting dates also will be posted on the Office of Compliance and Enterprise Risk Management's webpage.

VII. MTSU Corporate Compliance Plan

The purpose of the Corporate Compliance Plan (Plan) is to promote the University’s mission, strategic goals, and community standards of conduct in all operational, academic, and advancement activities and functions. Implementation of the Plan additionally will support the Institution’s efforts to assure compliance with all applicable state, federal, local, and accreditation regulations, laws, rules, standards, and obligations.

The following are the ways the Plan will serve as guidance to achieve the promotion and support of enterprise-wide compliance activities:

- ❖ Continuing education of MTSU Board of Trustees (Trustees) and Executive Officers regarding their fiduciary responsibility of annual review of the Plan.

- ❖ Continued establishment and review of policies and procedures related to University operations, academic performance, and ethics requirements.

- ❖ Training and education on policies and procedures to ensure understanding and adherence.

- ❖ Annual compliance and risk assessment audits, or more frequently as needed, to ensure compliance with state, federal, and local obligations.

- ❖ Maintenance of exisiting methods of confidentially reporting suspected fraud, waste, and abuse, including violations of MTSU policies, and the creation of additional confidential reporting methods to assure prompt investigation of all credible reports.

- ❖ Regular and systematic communication of MTSU compliance policies and procedures to the campus community.

- ❖ Dissemination and application of appropriate investigatory and disciplinary measures to address and/or to correct instances of noncompliance with Unversity policies and procedures.

A copy of the Corporate Compliance Plan can be found on the Office of Compliance and Enterprise Risk Management's website.

VIII. Risk Management and Compliance Resources

The University's risk management and compliance resources include:

- ❖ Annual Risk Assessment Plans by Institutional Division
- ❖ Institution Regulatory Compliance Matrix
- ❖ Risk Assessment Grid
- ❖ Corporate Compliance Committee
- ❖ Auditing and Consulting Services
- ❖ Mandatory training on certain regulatory topics
- ❖ E-Training presentations on risk management and compliance topics

IX. State Reporting

The University submits its risk assessments to the Comptroller of the State of Tennessee annually by December 31 to comply with the Financial Integrity Act (T.C.A. § 9-8-104).

Annually, two MTSU divisions at a time complete the COSO Enterprise Risk Management Framework Risk Assessment Forms (COSO Forms) to assess department/division risks and to review internal controls. The State of Tennessee began offering the use of the COSO Forms to institutions in 2017. Prior to the use of the COSO Forms, MTSU utilized the Crawford Model for risk assessment and review of internal controls.

APPENDIX A – Glossary of Terms

Risk. Any event, action, or issue that impacts the operations, mission, objectives, or student services of Middle Tennessee State University, or that has a likelihood of impact.

Risk Management. The process of developing plans involving assessment, communication, response, and monitoring to reduce the likelihood and/or impact of risk events, actions, or issues.

Enterprise Risk Management. A global, structured, and continuous approach to risk management that integrates control processes for risk identification, assessment, mitigation, and response across all areas of the Institution. ERM also ensures regular and adequate reporting for use in decision-making across all divisions of the University.

Risk Philosophy. A statement of the University's overall intentions, processes, and approach to assessing, accepting, avoiding, and mitigating enterprise-wide risk.

Risk Tolerance (Appetite). The amount of risk the Institution is willing to accept in order to meet its operational, strategic, and academic performance objectives. Risk tolerance or appetite also depends on corporate culture and may change over time as different risk arise or are mitigated.

Corporate Compliance. Programming across all areas of an organization or corporation that includes education, training, auditing, and continuous monitoring to assist in the detection and deterrence of unethical behavior or illegal activity by its employees, stakeholders, or corporate officers.

Control Activity. A process or action designed to provide reasonable assurance of achieving an objective, goal, or risk reduction.

APPENDIX B – References

1. United States Government Accountability Office, *Standards for Internal Control in the Federal Government (Green Book)*, GAO-14-704G (2014), *available at* https://www.gao.gov.

2. Financial Integrity Act of 1983, Tenn. Code Ann. § 9-18-101, et seq.

3. State of Tennessee, Department of Finance & Administration, Risk Management, *available at* https://www.tn.gov/finances/section/fa-accounts-risk-management.

4. State of Tennessee, Department of Finance & Administration, Optional Use Toolset, *available at* https://www.tn.gov.finance/topic/fa.accounts-optional-use-toolset.

5. Higher Education Compliance Alliance, *Compliance Matrix*, *available at* www.higheredcompliance.org/matrix/.

6. Andrea Falcione and Seth Cohen, *State of Compliance Study 2016*, PwC, *available at* https://www.pwc.com/us/en/risk-assurnace/state-of-compliance-study/assets/state-of-compliance-study-2016.pdf.

7. United States Sentencing Commission, *Sentencing of Organizations,* Effective Compliance and Ethics Program §8B2.1 (2015), *available at* https://www.ussc.gov/guidelines/2015-guidelines-manual/2015/chapter-8.