Middle Tennessee State University
Audit and Compliance Committee

10:00am CDT
Tuesday
September 12, 2017

Middle Tennessee State University
Student Union Building
1301 East Main St.
Murfreesboro, Tennessee 37132

Middle Tennessee State University
Audit and Compliance Committee

Tuesday, September 12, 2017 – 10:00am

ORDER OF BUSINESS

Call to Order

Roll Call

Remarks by Board Chairperson / President

Revised Audit Charter for Audit and Compliance Committee (Action) ..... Tab 1

Results of Prior State Audit Reports (Information)..... Tab 2

Annual Report – Audit and Consulting Services (Information) ..... Tab 3

Compliance and Enterprise Risk Management (Information)

a. United States Sentencing Guidelines: – Effective Compliance and Ethics Programs ..... Tab 4

b. Department of Justice "Filip Factors" – Evaluation of Corporate Compliance Programs ..... Tab 5

c. Green Book to COSO ERM Mapping ..... Tab 6

d. Compliance and ERM Overview and Activities ..... Tab 7

e. Financial Integrity Act and State Risk Assessment Reporting ..... Tab 8

Non-Public Executive Session – Discussion of Risk Assessments (Confidential Materials); and, Audits and Investigations (Information)

Public Session - Risk Assessment Report Submittal (Action) ..... Tab 9

Other Business

Adjourn

Middle Tennessee State University
Audit and Compliance Committee

Tuesday, September 12, 2017 – 10:00am

Tab 1

Revised Audit Charter for Audit and Compliance Committee

Middle Tennessee State University
Board of Trustees

MEETING:	Audit and Compliance Committee
SUBJECT:	*Revised Audit Charter for Audit and Compliance Committee*
DATE:	September 12, 2017
PRESENTER:	Brenda Burkhart
ACTION:	Voice Vote
STAFF RECOMMENDATION:	Approval

BACKGROUND INFORMATION:

The Audit Charter for the Audit and Compliance Committee requires approval from the Comptroller of the Treasury. After submission of the original Charter, the Comptroller directed that two sections of the Charter be revised in order to comply with the Comptroller's Guidelines for Audit Committee Charters.

Section V. Independence was revised to specifically state that members of the Audit and Compliance Committee "shall be free of any interests, in fact or in appearance, that are in conflict with their duties as members of the Audit and Compliance Committee" instead of referencing compliance with the Board Bylaws and Code of Ethics policy.

Section VI. Membership was revised to specifically state that "the chair of the Audit and Compliance Committee shall be appointed by the Board Chair and serve a one (1) year term," and "Appointments of the Audit and Compliance Committee members and its chair shall be approved by the Board."

The Audit Charter was also revised to reflect the change in title of the Director of Audit and Consulting Services to Chief Audit Executive.

The revised Audit Charter is recommended for approval.

Middle Tennessee State University

Audit and Compliance Committee Charter

I. Purpose

The Audit and Compliance Committee, a standing committee of the Middle Tennessee State University Board of Trustees (Board), will assist the Board in exercising oversight of the University's financial and accounting practices, internal controls, risk assessments and standards of conduct.

II. Mission

The Audit and Compliance Committee will provide oversight of the following areas:

A. Audit engagements with the Tennessee Comptroller's Office, including the integrity of financial statements and compliance with legal and regulatory requirements,
B. Audit engagements with external auditors,
C. Internal Audit activities,
D. Internal Audit administration,
E. Internal controls and compliance with laws, regulations, and other requirements,
F. Risk and control assessments,
G. Fraud, waste, and abuse prevention, detection, and reporting, and
H. Other areas as directed by the Board.

III. Authority

The Audit and Compliance Committee has the authority to authorize or facilitate audits or investigations into any matter within its scope of responsibility. The Committee is authorized to:

A. Seek any information it requires from employees or external parties. Employees are directed to cooperate with the Committee's requests,
B. Meet with Board and institutional officials, external and internal auditors, legal counsel, or others as necessary, and
C. Oversee the University's internal audit function.

IV. Responsibilities

The Audit and Compliance Committee has responsibilities for the following:

A. Tennessee Comptroller's Office Audits (State Auditors)
    1. Understand the scope and approach used by the State Auditors in conducting their examinations,
    2. Review results of the Comptroller's examinations of financial statements and any other matters related to the conduct of the audits,

3. Review with management and legal counsel any legal matters (including pending litigation) that may have a material impact on the financial statements, and any material reports or inquiries from regulatory or governmental agencies,
4. Ensure that the Comptroller is notified of any indications of fraud in the manner prescribed by the Comptroller,
5. Resolve any differences between management and the Comptroller's auditors regarding financial reporting, and
6. Meet, as needed, with the Comptroller's auditors to discuss any matters that the Audit and Compliance Committee or State Auditors deem appropriate.

B. External Audits
1. Understand the scope and approach used by the external auditors in conducting their examinations,
2. Review results of the external auditors' examinations and any other matters related to the conduct of the external audits, and
3. Meet, as needed, with the external auditors to discuss any matters that the Audit and Compliance Committee or external auditors deem appropriate.

C. Internal Audit (Audit and Consulting Services)
1. Ensure that the Chief Audit Executive reports directly to the Audit and Compliance Committee and has direct and unrestricted access to the chair of the Audit and Compliance Committee,
2. Review and approve the internal audit charter for the University's department of Audit and Consulting Services,
3. Review and approve the annual audit plans for the University's department of Audit and Consulting Services, including management's request for unplanned audits,
4. Receive and review significant results of internal audits performed,
5. Work with University management and Audit and Consulting Services to assist with the resolution of cooperation issues and to ensure the implementation of audit recommendations,
6. Review the results of the year's work with the Chief Audit Executive, and
7. Ensure the University's internal audit function maintains a quality assurance and improvement program, including internal procedures and assessments and a periodic external quality assessment of conformance with the Institute of Internal Auditors' *International Standards for the Professional Practice of Internal Auditing.*

D. Internal Audit Administration
1. Ensure the Chief Audit Executive's administrative reporting relationship to the President is independent.
2. Ensure that Audit and Consulting Services has adequate resources in terms of staff and budget to effectively perform its responsibilities.
3. Review and approve the appointment and compensation of the Chief Audit Executive,
4. Recommend to the Board dismissal of the Chief Audit Executive only for cause

5. Review and approve the compensation and termination of campus internal auditors.

E. Risk, Internal Control and Compliance
   1. Consider the effectiveness of the internal control system and compliance with laws and regulations, including computerized information system controls and security,
   2. Review and evaluate risk assessments performed by institutional management and the Board, and
   3. Inform the Comptroller of the Treasury of the results of risk assessments and controls completed by University management.

F. Fraud
   1. Ensure that the Board and the University have an effective process in place to prevent, detect, and report fraud, waste and abuse.
   2. Facilitate audit and investigative matters, including advising auditors and investigators of any pertinent information received by the Audit and Compliance Committee.

G. Other
   1. Review and assess the adequacy of the Audit and Compliance Committee's charter every four years or as needed, whichever is earlier, requesting Board approval for any proposed changes.
   2. Ensure there are procedures for the receipt, retention, and treatment of complaints about accounting, internal controls, or auditing matters.
   3. Review the University's code of conduct and/or policies regarding employee conduct to ensure that they are easy to access, are widely distributed, are easy to understand and implement, include a confidential mechanism for reporting code violations, are enforced, and include a conflict of interest policy.
   4. Review the University's conflict of interest policy to ensure that the term "conflict of interest" is clearly defined, the policy is comprehensive, annual signoff is required, and potential conflicts are adequately resolved and documented.

V. Independence

The members of the Audit and Compliance Committee shall be free of any interests, in fact or in appearance, that are in conflict with their duties as members of the Audit and Compliance Committee.

VI. Membership

A. Pursuant to TCA 4-35-104, the Audit and Compliance Committee shall have at least three voting members,
B. The Audit and Compliance Committee members shall be appointed by the Board Chair and serve a two (2) year term,
C. The chair of the Audit and Compliance Committee shall be appointed by the Board Chair and serve a one (1) year term,

D. Appointments of the Audit and Compliance Committee members and its chair shall be approved by the Board,
E. The Board Chair shall serve as an ex officio Voting member of the Audit and Compliance Committee,
F. The Audit and Compliance Committee shall include at least one member, the chair of the committee, who shall have accounting and financial management expertise, and
G. The other members of the Audit and Compliance Committee shall be generally knowledgeable in financial, management, and auditing matters.

VII. Meetings

A. The Audit and Compliance Committee shall meet at least quarterly during each calendar year, and may meet more frequently as deemed necessary. Meetings may be requested by the Board Chair, chair of the Audit and Compliance Committee or the Comptroller of the Treasury,
B. The Audit and Compliance Committee may invite Board management, auditors, or others to attend and provide relevant information,
C. Minutes shall be made of all meetings of the Audit and Compliance Committee and provided to the Board Chair, the President of the University and the Secretary to the Board. The minutes shall be maintained as the official record of such meetings,
D. A majority of the voting members of the committee shall constitute a quorum for the transaction of business.
E. All meetings of the Audit and Compliance Committee shall adhere to the Open Meetings Act, Tennessee Code Annotated Title 8, Chapter 44, except that pursuant to TCA Section 4-35-108(b), the Audit and Compliance Committee may hold confidential, nonpublic executive sessions for the sole purpose of discussing the following:
    1. Items deemed not subject to public inspection under Tennessee Code Annotated, Sections 10-7-503 and 10-7-504, and all other matters designated as confidential or privileged under state or federal law,
    2. Litigation,
    3. Audits or investigations, and
    4. Matters involving information under Tennessee Code Annotated, Section 4-35-107(a), where the informant has requested anonymity.

Approvals

Approved by: _____ Date: _____
[Name]
Chair of the Audit Committee

Approved by: _____ Date: _____
[Name]
Chairman of the Board

Middle Tennessee State University
Audit and Compliance Committee

Tuesday, September 12, 2017 – 10:00am

Tab 2

Results of Prior State Audit Reports

Middle Tennessee State University
Board of Trustees

MEETING:	Audit and Compliance Committee
SUBJECT:	*Results of Prior State Audit Reports*
DATE:	September 12, 2017
PRESENTER:	Brenda Burkhart
ACTION:	Information Item

BACKGROUND INFORMATION:

The list of Results from State Audit Reports for the Past 15 Years (2002 – 2016) is an information item requested by the Audit and Compliance Committee. In the past 15 years, there were four audit findings. One finding in 2009 pertained to foundation accounting and the other three findings pertained to information technology internal control weaknesses considered confidential pursuant to TCA 10-7-504(i). Management implemented corrective action and there were no repeat audit findings.

Results from State Audit Reports for the Past 15 Years (2002 - 2016)

Count	Audit Objectives Defined, See Notes	State Audit Report	Opinion on Financial Statements	Results - Audit Findings
1	A	FYE June 30, 2016	Unmodified	None
2	A	FYE June 30, 2015	Unmodified	One Finding, see (1)
3	A	FYE June 30, 2014	Unmodified	One Finding, see (2)
4	A	FYE June 30, 2013	Unmodified	None
5	B	FYE June 30, 2012	Unqualified	None
6	B	FYE June 30, 2011	Unqualified	None
7	B	FYE June 30, 2010	Unqualified	None
8	B	FYE June 30, 2009	Unqualified	One Finding, see (3)
9	B	FYE June 30, 2008	Unqualified	None
10	B	FYE June 30, 2007	Unqualified	None
11	B	FYE June 30, 2006	Unqualified	One Finding, see (4)
12	B	FYE June 30, 2005	Unqualified	None
13	B	FYE June 30, 2004	Unqualified	None
14	B	FYE June 30, 2003	Unqualified	None
15	B	FYE June 30, 2002	Unqualified	None

Notes - Audit Objectives:

A To express opinions on the financial statements based on the audit but no opinion expressed on the effectiveness of the entity's internal controls.

B The objectives of the audit were to consider the university's internal control over financial reporting; to determine compliance with certain provisions of laws, regulations, contracts, and grant agreements; to determine the fairness of the presentation of the financial statements; and to recommend appropriate actions to correct any deficiencies.

Footnotes - Title of Audit Findings:

For each finding, management implemented corrective action. No repeat findings.

(1) 2015 - The University did not provide adequate internal controls in three specific areas. The details are confidential pursuant to TCA 10-7-504(i). (Concern was IT Controls)

(2) 2014 - The University did not provide adequate internal controls in one specific area. We observed a condition that was in violation of industry-accepted best practices. The details are confidential pursuant to TCA 10-7-504(i). (Concern was System Access)

(3) 2009 - The University did not ensure that amounts were properly reported in the Foundation's financial statements and accompanying notes to the financial statements. (Concern was Foundation Accounting)

(4) 2006 - MTSU and TBR should improve information security controls related to the SunGard HE Banner system implementation and maintenance. The details are confidential pursuant to TCA 10-7-504(i). (Concern was Software Design)

Middle Tennessee State University
Audit and Compliance Committee

Tuesday, September 12, 2017 – 10:00am

Tab 3

Audit and Consulting Services
Annual Report
Fiscal Year 2017

Middle Tennessee State University
Board of Trustees

MEETING:	Audit and Compliance Committee
SUBJECT:	*2017 Annual Report for Audit and Consulting Services*
DATE:	September 12, 2017
PRESENTER:	Brenda Burkhart
ACTION:	Information Item

BACKGROUND INFORMATION:

TCA 49-14-102 along with the MTSU Board of Trustees Bylaws and Policy on Board Committees requires a comprehensive report on the internal audit function to include the status of the 2017 annual audit plan noting the audits completed, in progress and scheduled but not completed. The report also includes an update on fraud awareness efforts and investigations along with the financial resources for Audit and Consulting Services.

As required, the Audit and Consulting Services Annual Report for Fiscal Year 2017 is submitted to the Audit and Compliance Committee for review.

MIDDLE TENNESSEE STATE UNIVERSITY

Audit and Consulting Services

Annual Report
Fiscal Year 2017

Audit and Consulting Services
Middle Tennessee State University
Murfreesboro, TN 37132

Audit and Consulting Services
Middle Tennessee State University
1301 East Main Street
Murfreesboro, TN 37132
Office: 615-898-2914 • Fax: 615-904-8046

MIDDLE TENNESSEE STATE UNIVERSITY

August 30, 2017

MTSU Board of Trustees
Audit and Compliance Committee

and

Dr. Sidney A. McPhee, President
Middle Tennessee State University
1301 East Main Street
Murfreesboro, TN 37132

Trustees and Dr. McPhee:

Enclosed is the annual report for Audit and Consulting Services for the 2017 fiscal year. An annual report of audit work is required by TCA 49-14-102 and the Bylaws and Policies of the MTSU Board of Trustees. The Board Committee policy requires a comprehensive report on the internal audit function to the Board through the Audit and Compliance Committee at a stated meeting. The report includes the status of the 2017 annual audit plan noting the audits completed, in progress, and scheduled but not completed.

The report also includes an update on the fraud awareness activities and investigations along with a report of the financial resources of Audit and Consulting Services.

This report fulfills the annual reporting requirements and provides information to the Board of Trustees concerning the 2017 audit efforts of Audit and Consulting Services. This report is intended solely for the internal use of Middle Tennessee State University and the MTSU Board of Trustees. It is not intended to be and should not be used for any other purpose. The distribution of the report to external parties should be approved by the Office of Audit and Consulting Services at Middle Tennessee State University.

Respectfully submitted,

Brenda H. Burkhart

Brenda H. Burkhart, CPA
Chief Audit Executive

Middle Tennessee State University
Audit and Consulting Services

Annual Report for Fiscal Year 2017

TABLE OF CONTENTS

MIDDLE TENNESSEE STATE UNIVERSITY
AUDIT AND CONSULTING SERVICES

ANNUAL REPORT FOR FISCAL YEAR 2017

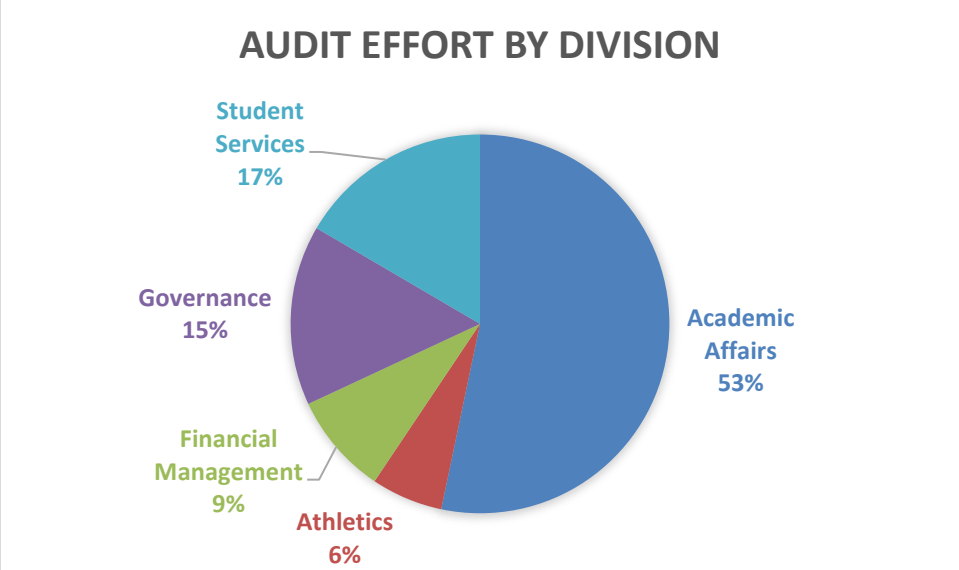
INTRODUCTION

Fiscal Year 2017 was a year of transition for Audit and Consulting Services. Audit and Consulting Services assisted with the University's efforts to transition from governance by the Tennessee Board of Regents (TBR) to governance by the MTSU Board of Trustees with the passage of the Focus on College and University Success (FOCUS) Act on April 2016. This transition process required the review of all policies, procedures and processes. The Director of Audit and Consulting Services served as a member of the Focus Act Transition Team and assisted with the review of all TBR and University policies and procedures. The audit staff also assisted with the policy review process.

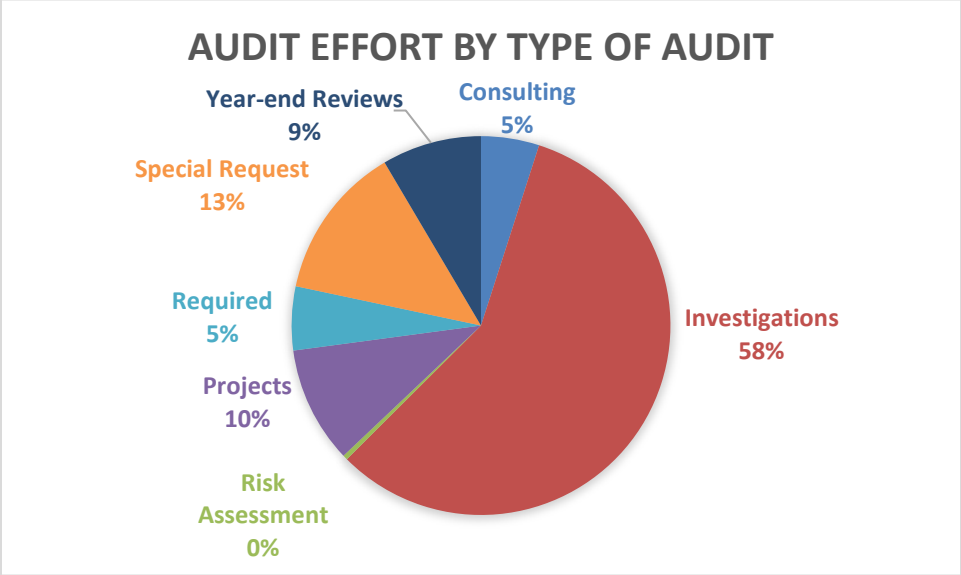
On April 10, 2017 the MTSU Board of Trustees was charged with governance of the University and the Audit and Compliance Committee was charged with oversight of the internal audit function of Audit and Consulting Services.

AUDIT EFFORT

Audit and Consulting Services tracks audit effort by type of project and by university division as shown with the following charts. For the chart Audit Effort by Division, Governance includes the President's Division and general institutional support. The majority of audit effort (70%) focused on projects within Academic Affairs and Student Services. The Governance audit effort (15%) included the work with the FOCUS transition team.



The type of audit work performed is defined by the source of the request or purpose of the audit work. Investigations represented 58% of the audit effort. Investigations began as a result of management referral of concerns of possible fraud, waste or abuse or a hotline complaint of possible improper or dishonest acts. Projects (10%) included the completion of an internal peer review and the audit effort with the FOCUS Act transition team. Consulting and Special Request (18%) represented efforts responding to general questions, assisting with the reporting of president's expenses or assisting management with an audit concern. Required projects (5%) are the result of a third party request or agreement that an audit or review be performed. This audit effort included the annual audit of Football Ticket Sales and Paid Attendance required by the National Collegiate Athletic Association (NCAA) and audit effort assisting the State Auditors. Year-end Reviews consisted of inventory observations and cash counts at the end of the fiscal year.



The Status of Internal Audit Plan for Fiscal Year Ending June 30, 2017 is located on the next page and lists completed projects and projects in progress. There were three projects scheduled but not completed due to the audit effort used for investigations. These projects will be scheduled for the 2018 fiscal year.

Middle Tennessee State University
Status of Internal Audit Plan
Fiscal Year Ending June 30, 2017

Type	Area	Audit	Current Status
P	GV	Internal Peer Review FY2016	Completed
P	GV	Project-FOCUS	Completed
R	FM	State Audit FY2016, Assistance/Follow-up	Completed
R	AT	Football Attendance 2016	Completed
Y	FM	Cash Counts FY2016	Completed
Y	FM	Inventories FY2016	Completed
C	GV	Assistance - President's Expenses	Completed
C	GV	General Consultation/Research	Completed
I	SS	INV1402	Completed
I	FM	INV1501	Completed
I	GV	INV1502	Completed
I	AA	INV1504	Completed
I	AA	INV1506	Completed
I	SS	INV1601	Completed
I	SS	INV1602	In Progress
I	AA	INV1604	In Progress
I	AA	INV1701	In Progress
I	SS	INV1702	In Progress
I	AT	INV1703	In Progress
I	MC	INV1704	In Progress
I	AA	INV1705	In Progress
M	GV	Management Risk Assessment	In Progress
S	AA	Confucius Institute	In Progress
Y	FM	Cash Counts FY2017	In Progress
Y	FM	Inventories FY2017	In Progress
A	AA	Research Services Procedural Review	Scheduled
A	SS	Financial Aid Procedural Review	Scheduled
F	FM	Follow-up Reviews as Needed	Scheduled

Audit Types:

A - Risk-Based (Assessed)
C - Consulting
F - Follow-up Review
I - Investigation
M - Management's Risk Assessment
P - Project (Ongoing or Recurring)
R - Required
S - Special Request
Y - Year-end Reviews

Area = University Division

AA - Academic Affairs
AD - Advancement
AT - Athletics
FM - Financial Management
GV - Governance/Executive Office
IT - Information Technology
MC - Marketing and Communications
SS - Student Services

FRAUD AWARENESS

The University is committed to the responsible stewardship of resources, and is required by state law to provide a means by which employees, students or others may report suspected or known improper or dishonest acts. Audit and Consulting Services manages the reporting process by which students, employees, taxpayers or other citizens may confidentially report suspected illegal, improper, wasteful or fraudulent activity. (TCA 49-14-103)

The "Fraud Awareness" brochure was revised and updated to reflect the University's governance change to the MTSU Board of Trustees. This brochure is a communication tool given to new employees that explains the reporting expectations and options for any individual that suspects known improper or dishonest acts involving university employees, outside contractors or vendors. The "Fraud Awareness" information was also revised and updated on the Audit and Consulting Services webpage to include an on-line reporting form.

When Audit and Consulting Services receives allegations of improper or dishonest acts by an employee, outside contractor or vendor, it is required to conduct an investigation. The purpose of the investigation or review is to determine if the allegation or concern is substantiated or unsubstantiated and if there are any internal control weaknesses or risks that management should address. If the allegation or concern is substantiated and corrective action is needed, an audit report is issued. A review is administratively closed with a memo to the file if the concern is unsubstantiated or referred to management or there are no recommendations for corrective action.

Below is a summary of the reviews pertaining to concerns of possible improper or dishonest acts:

Reviews brought forward from prior year	8
New reviews opened during year	5
Reviews administratively closed	5
Reports Issued	1
Reviews in Progress at June 30, 2017	7

In 2017, five new reviews of possible improper or dishonest acts were opened which is one more than the three year average of four reviews per year. New reviews for the past three years were: 4 in 2016; 6 in 2015; and 2 in 2014.

The report issued concerned the special review of an education abroad program to Athens, Greece in May 2015. The complaint stated the housing budget was inflated and generated excess funds that were not accounted for properly. The complaint concerning student housing expenses was unsubstantiated but recommendations were made to address policy concerns noted during the review. The travel documentation contained duplicate receipts and errors totaling $1,994.21 which was repaid by the faculty member. Recommendations were made as follows: student enrollment and payment requirements should be met; faculty should be adequately trained for managing education abroad courses; and travel expense documentation including the translation of receipts should be improved. Management agreed to corrective action.

RESOURCES

As defined in the MTSU Audit and Compliance Committee Charter, the Audit and Compliance Committee is responsible for ensuring Audit and Consulting Services has adequate resources in terms of staff and budget to effectively perform its responsibilities. The following is the estimated budget for 2017-2018 compared to the actual expenses of the prior two fiscal years.

	Estimated Budget (1) 2017-2018	Actual Expenses 2016-2017	Actual Expenses 2015-2016
Salaries:			
Chief Audit Executive	$ 103,050	$ 83,744	$ 82,628
Assistant Director	61,400	60,305	59,362
Internal Auditors, 2 Professionals	85,555	84,136	82,386
Support Staff includes Longevity	26,802	26,148	25,256
Longevity for Professional Staff	7,800	7,600	7,400
Benefits	134,484	132,954	123,548
Total Salaries and Benefits	$ 419,091	$ 394,887	$ 380,580
Travel	7,500	11,272	14,330
Operating Expenses	15,583	4,406	4,100
Total Budget/Expenses	$ 442,174	$ 410,565	$ 399,010
Other Funding:			
Carry Forward from Prior Audit Services Revenue (2)	$ 32,848	$ 36,620	$ 43,450

(1) Estimated budget for FY 2017-2018. Budget will be finalized in October 2017.

(2) At June 30, 2015 audit services contracts with two community colleges ended with generated revenue of $43,450. The revenue was designated to fund conference/training travel for the auditors. Each year the unspent funds are carried forward to the next fiscal year.

The 2017-2018 budget for Audit and Consulting Services is adequate to fulfill the current responsibilities. There are no additional budget requests at this time.

AUDIT PLAN FOR FISCAL YEAR 2018

The projects in progress at June 30, 2017 along with the projects scheduled but not completed have been added to the approved audit plan for 2018 presented on the next page.

Middle Tennessee State University
Internal Audit Plan
Fiscal Year Ended June 30, 2018
Updated August 31, 2017

Type	Area	Audit	Current Status
I	SS	INV1602	In Progress
I	AA	INV1604	In Progress
I	AA	INV1701	In Progress
I	SS	INV1702	In Progress
I	AT	INV1703	In Progress
I	MC	INV1704	In Progress
I	AA	INV1705	In Progress
M	GV	Management Risk Assessment	In Progress
S	AA	Confucius Institute	In Progress
Y	FM	Cash Counts FY2017	In Progress
Y	FM	Year-End Inventory FY2017	In Progress
R	GV	Audit of President's Office	Scheduled
R	AT	Football Attendance Fall 2017	Scheduled
F	FM	State Audit Assistance/Follow-Up	Scheduled
C	GV	General Consultation	Scheduled
F	GV	Follow-up, Prior Recommendations	Scheduled
I	GV	Unscheduled Investigations	Scheduled
Y	FM	Cash Counts FY2018	Scheduled
Y	FM	Year-End Inventory FY2018	Scheduled
A	AA	Research Services Procedural Review	Scheduled
A	SS	Financial Aid Procedural Review	Scheduled
A	FM	Property Management Contract Review	Scheduled

Audit Types:

A - Risk-Based (Assessed)
C - Consulting
F - Follow-up Review
I - Investigation
M - Management's Risk Assessment
P - Project (Ongoing or Recurring)
R - Required
S - Special Request
Y - Year-end Reviews

Area = University Division

AA - Academic Affairs
AD - Advancement
AT - Athletics
FM - Financial Management
GV - Governance/Executive Office
IT - Information Technology
MC - Marketing and Communications
SS - Student Services

Middle Tennessee State University
Audit and Compliance Committee

Tuesday, September 12, 2017 – 10:00am

Tab 4

United States Sentencing Guidelines: Effective Compliance and Ethics Programs

Middle Tennessee State University
Board of Trustees

MEETING:	Audit and Compliance Committee
SUBJECT:	*United States Sentencing Guidelines – Effective Compliance and Ethics Programs*
DATE:	September 12, 2017
PRESENTER:	Gené Stephens
ACTION:	None

BACKGROUND INFORMATION:

In 1991, the United States Sentencing Commission ("Commission") implemented guidelines to help companies detect and prevent criminal activity as a way of mitigating fines and sanctions The guidelines outlined seven (7) elements for developing and maintaining an effective corporate compliance and ethics program (U.S. Sentencing Commission Guidelines Manual § 8D1.4). The following summarizes the Commission's guidelines for designing and maintaining an effective compliance and ethics program ("the program"):

1. Establish standards and procedures.
2. Ensure oversight and accountability of the program by the organization's governing authority (i.e. the Board of Trustees).
3. Perform due diligence in hiring and promoting individuals to ensure they have not engaged in prior illegal activities or conduct inconsistent with the organization's standards.
4. Provide training and communication regarding the program.
5. Monitor, audit, and report compliance and ethics issues
6. Enforce discipline and provide appropriate incentives for following standards.
7. Respond to, and prevent, criminal conduct.

In 2015, an additional, eighth element was added to the above guidelines to incorporate the use of periodic risk assessments.

The Commission's guidelines are provided for the Board's review and are being utilized by the University to further develop and strengthen the institution's corporate compliance and risk management program.

§8D1.4 (Recommended Conditions of Probation - Organizations), an organization shall—

(1) exercise due diligence to prevent and detect criminal conduct; and

(2) otherwise promote an organizational culture that encourages ethical conduct and a commitment to compliance with the law.

Such compliance and ethics program shall be reasonably designed, implemented, and enforced so that the program is generally effective in preventing and detecting criminal conduct. The failure to prevent or detect the instant offense does not necessarily mean that the program is not generally effective in preventing and detecting criminal conduct.

(b) Due diligence and the promotion of an organizational culture that encourages ethical conduct and a commitment to compliance with the law within the meaning of subsection (a) minimally require the following:

(1) The organization shall establish standards and procedures to prevent and detect criminal conduct.

(2) (A) The organization's governing authority shall be knowledgeable about the content and operation of the compliance and ethics program and shall exercise reasonable oversight with respect to the implementation and effectiveness of the compliance and ethics program.

(B) High-level personnel of the organization shall ensure that the organiza-tion has an effective compliance and ethics program, as described in this guideline. Specific individual(s) within high-level personnel shall be assigned overall responsibility for the compliance and ethics program.

and, as appropriate, to the governing authority, or an appropriate subgroup of the governing authority, on the effective¬ness of the compliance and ethics program. To carry out such operational responsibility, such individual(s) shall be given adequate resources, appropriate authority, and direct access to the governing authority or an appropriate subgroup of the governing authority.

(3) The organization shall use reasonable efforts not to include within the substantial authority personnel of the organization any individual whom the organization knew, or should have known through the exercise of due diligence, has engaged in illegal activities or other conduct inconsistent with an effective compliance and ethics program.

(4) (A) The organization shall take reasonable steps to communicate periodi¬cally and in a practical manner its standards and procedures, and other aspects of the compliance and ethics program, to the individuals referred to in subparagraph (B) by conducting effective training programs and otherwise disseminating information appropriate to such individuals' respective roles and responsibilities.

(B) The individuals referred to in subparagraph (A) are the members of the governing authority, high-level personnel, substantial authority personnel, the organization's employees, and, as appropriate, the organization's agents.

(5) The organization shall take reasonable steps—

(A) to ensure that the organization's compliance and ethics program is followed, including monitoring and auditing to detect criminal conduct;

mechanisms that allow for anonymity or confidentiality, whereby the organization's employees and agents may report or seek guidance regarding potential or actual criminal conduct without fear of retaliation.

(6) The organization's compliance and ethics program shall be promoted and enforced consistently throughout the organization through (A) appropriate incentives to perform in accordance with the compliance and ethics program; and (B) appropriate disciplinary measures for engaging in criminal conduct and for failing to take reasonable steps to prevent or detect criminal conduct.

(7) After criminal conduct has been detected, the organization shall take reasonable steps to respond appropriately to the criminal conduct and to prevent further similar criminal conduct, including making any necessary modifications to the organization's compliance and ethics program.

(c) In implementing subsection (b), the organization shall periodically assess the risk of criminal conduct and shall take appropriate steps to design, implement, or modify each requirement set forth in subsection (b) to reduce the risk of criminal conduct identified through this process.

Commentary

Application Notes:

1. *Definitions.—For purposes of this guideline:*

"Compliance and ethics program" means a program designed to prevent and detect criminal conduct.

"Governing authority" means the (A) the Board of Directors; or (B) if the organization does not have a Board of Directors, the highest-level governing

An Overview of the Organizational Guidelines

Paula Desio, Deputy General Counsel, United States Sentencing Commission

Organizations, like individuals, can be found guilty of criminal conduct, and the measure of their punishment for felonies and Class A misdemeanors is governed by Chapter Eight of the sentencing guidelines. While organizations cannot be imprisoned, they can be fined, sentenced to probation for up to five years, ordered to make restitution and issue public notices of conviction to their victim and exposed to applicable forfeiture statutes. Data collected by the Sentencing Commission reflect that organizations are sentenced for a wide range of crimes. The most commonly occurring offenses (in order of decreasing frequency) are fraud, environmental waste discharge, tax offenses, antitrust offenses, and food and drug violations.

The organizational sentencing guidelines (which apply to corporations, partnerships, labor unions, pension funds, trusts, non-profit entities, and governmental units) became effective November 1, 1991, after several years of public hearings and analyses. These guidelines are designed to further two key purposes of sentencing: "just punishment" and "deterrence." Under the "just punishment" model, the punishment corresponds to the degree of blameworthiness of the offender, while under the "deterrence" model, incentives are offered for organizations to detect and prevent crime.

Effective Compliance Programs

Criminal liability can attach to an organization whenever an employee of the organization commits an act within the apparent scope of his or her employment, even if the employee acted directly contrary to company policy and instructions. An entire organization, despite its best efforts to prevent wrongdoing in its ranks, can still be held criminally liable for any of its employees' illegal actions. Consequently, when the Commission promulgated the organizational guidelines, it attempted to alleviate the harshest aspects of this institutional vulnerability by incorporating into the sentencing structure the preventive and deterrent aspects of systematic compliance programs. The Commission did this by mitigating the potential fine range - in some cases up to 95 percent - if an organization can demonstrate that it had put in place an effective compliance program. This mitigating credit under the guidelines is contingent upon prompt reporting to the authorities and the non-involvement of high level personnel in the actual offense conduct.

Chapter Eight outlines seven key criteria for establishing an "effective compliance program":

Compliance standards and procedures reasonably capable of reducing the prospect of criminal activity—

- Oversight by high-level personnel
- Due Care in delegating substantial discretionary authority
- Effective Communication to all levels of employees
- Reasonable steps to achieve compliance, which include systems for monitoring, auditing, and reporting suspected wrongdoing without fear of reprisal
- Consistent enforcement of compliance standards including disciplinary mechanisms
- Reasonable steps to respond to and prevent further similar offenses upon detection of a violation

The organizational guidelines criteria embody broad principles that, taken together, describe a corporate "good citizenship" model, but do not offer precise details for implementation. This approach was deliberately selected in order to encourage flexibility and independence by organizations in designing programs that are best suited to their particular circumstances.

Sharing "Best Practices" Ideas

The innovative approach put forward in the sentencing guidelines has spawned complementary efforts by a number of regulatory and law enforcement authorities, Executive agencies such as the Environmental Protection Agency, the Department of Health and Human Services, and the Department of Justice's Antitrust Division have developed, or are developing model compliance programs, programs for self-reporting, and programs for amnesty - all of which are modeled after some aspect of the organizational sentencing guidelines. Industry and peer organizations are forming to share ideas on "best practices" for compliance training and ethics awareness.

The Commission will continue to study the effectiveness of these efforts to implement the compliance criteria of Chapter Eight. In particular, the Commission is interested in assessments of the viability of its efforts to encourage organizations - from large corporations to non-profits organizations to governmental units - to develop institutional cultures that discourage criminal conduct. ■

For more information, contact the United States Sentencing Commission, One Columbus Circle, N.E., Suite 2-500, Washington, DC 20002-8002.
Phone: 202-502-4500; FAX: 202-502-4699

Middle Tennessee State University
Audit and Compliance Committee

Tuesday, September 12, 2017 – 10:00am

Tab 5

Department of Justice "Filip Factors" – Evaluation of Corporate Compliance Programs

Middle Tennessee State University
Board of Trustees

MEETING:	Audit and Compliance Committee
SUBJECT:	*Department of Justice "Filip Factors" – Evaluation of Corporate Compliance Programs*
DATE:	September 12, 2017
PRESENTER:	Gené Stephens
ACTION:	None

BACKGROUND INFORMATION:

The Fraud Section of the Department of Justice describes specific factors prosecutors consider in conducting an investigation of a corporate entity. The factors, known as "Filip Factors," state that the existence of a corporation's pre-existing compliance program, or its remedial efforts to improve upon an existing program, are factors considered in determining whether to bring charges against an organization and its officers or negotiate other agreements.

As part of the Filip Factors, the DOJ set forth questions considered relevant in their evaluation of an organization's corporate compliance program. The following are some of the topics covered by the DOJ's questions. The questions were issued in February 2017.

1. Root cause analysis of misconduct and remediation;
2. Senior and middle management's oversight and shared commitment to compliance;
3. Autonomy of the compliance role and resources provided for the role;
4. Design and implementation of policies and procedures;
5. Operational integration of the compliance policies and procedures;
6. Risk management and assessment;

7. Training, communication, and guidance availability;

8. Reporting and investigation;

9. Incentive and disciplinary measures; and

10. Continuous improvement, periodic testing, and review of the high risk areas.

The DOJ's factors and questions reiterate the importance of organizational implementation of an effective corporate compliance program. The information is provided for the Board's review to further demonstrate the significance of maintaining a system of internal compliance programming, as well as ongoing risk management and assessment activities, to prevent incidences of internal fraud, waste, abuse, and/or other criminal or questionable activities that are contrary to the University's stated mission and goals.

U.S. Department of Justice
Criminal Division
Fraud Section

Evaluation of Corporate Compliance Programs

Introduction

The Principles of Federal Prosecution of Business Organizations in the United States Attorney's Manual describe specific factors that prosecutors should consider in conducting an investigation of a corporate entity, determining whether to bring charges, and negotiating plea or other agreements. These factors, commonly known as the "Filip Factors," include "the existence and effectiveness of the corporation's pre-existing compliance program" and the corporation's remedial efforts "to implement an effective corporate compliance program or to improve an existing one."

Because a corporate compliance program must be evaluated in the specific context of a criminal investigation that triggers the application of the Filip Factors, the Fraud Section does not use any rigid formula to assess the effectiveness of corporate compliance programs. We recognize that each company's risk profile and solutions to reduce its risks warrant particularized evaluation. Accordingly, we make an individualized determination in each case.

There are, however, common questions that we may ask in making an individualized determination. This document provides some important topics and sample questions that the Fraud Section has frequently found relevant in evaluating a corporate compliance program. The topics and questions below form neither a checklist nor a formula. In any particular case, the topics and questions set forth below may not all be relevant, and others may be more salient given the particular facts at issue.

Many of the topics below also appear in the United States Attorney's Manual ("USAM"), in the United States Sentencing Guidelines ("USSG"), in Fraud Section corporate resolution agreements, in *A Resource Guide to the U.S. Foreign Corrupt Practices Act* ("FCPA Guide") published in November 2012 by the Department of Justice (DOJ) and the Securities and Exchange Commission (SEC), in the Good Practice Guidance on Internal Controls, Ethics, and Compliance adopted by the Organization for Economic Co-operation and Development ("OECD") Council on February 18, 2010, and in the Anti-Corruption Ethics and Compliance Handbook for Business ("OECD Handbook") published in 2013 by OECD, United Nations Office on Drugs and Crime, and the World Bank.

Sample Topics and Questions

1. Analysis and Remediation of Underlying Misconduct

- **Root Cause Analysis** – What is the company's root cause analysis of the misconduct at issue? What systemic issues were identified? Who in the company was involved in making the analysis?

- **Prior Indications** – Were there prior opportunities to detect the misconduct in question, such as audit reports identifying relevant control failures or allegations, complaints, or investigations involving similar issues? What is the company's analysis of why such opportunities were missed?

- ☐ **Remediation** – What specific changes has the company made to reduce the risk that the same or similar issues will not occur in the future? What specific remediation has addressed the issues identified in the root cause and missed opportunity analysis?

2. Senior and Middle Management[1]

☐ **Conduct at the Top** – How have senior leaders, through their words and actions, encouraged or discouraged the type of misconduct in question? What concrete actions have they taken to demonstrate leadership in the company's compliance and remediation efforts? How does the company monitor its senior leadership's behavior? How has senior leadership modelled proper behavior to subordinates?

☐ **Shared Commitment** – What specific actions have senior leaders and other stakeholders (*e.g.*, business and operational managers, Finance, Procurement, Legal, Human Resources) taken to demonstrate their commitment to compliance, including their remediation efforts? How is information shared among different components of the company?

☐ **Oversight** – What compliance expertise has been available on the board of directors? Have the board of directors and/or external auditors held executive or private sessions with the compliance and control functions? What types of information have the board of directors and senior management examined in their exercise of oversight in the area in which the misconduct occurred?

3. Autonomy and Resources[2]

☐ **Compliance Role** – Was compliance involved in training and decisions relevant to the misconduct? Did the compliance or relevant control functions (*e.g.*, Legal, Finance, or Audit) ever raise a concern in the area where the misconduct occurred?

☐ **Stature** – How has the compliance function compared with other strategic functions in the company in terms of stature, compensation levels, rank/title, reporting line, resources, and access to key decision-makers? What has been the turnover rate for compliance and relevant control function personnel? What role has compliance played in the company's strategic and operational decisions?

☐ **Experience and Qualifications** – Have the compliance and control personnel had the appropriate experience and qualifications for their roles and responsibilities?

- **Autonomy** – Have the compliance and relevant control functions had direct reporting lines to anyone on the board of directors? How often do they meet with the board of directors? Are members of the senior management present for these meetings? Who reviewed the performance of the compliance function and what was the review process? Who has determined compensation/bonuses/raises/hiring/termination of compliance officers? Do the compliance and relevant control personnel in the field have reporting lines to headquarters? If not, how has the company ensured their independence?

- **Empowerment** – Have there been specific instances where compliance raised concerns or objections in the area in which the wrongdoing occurred? How has the company responded to such compliance concerns? Have there been specific transactions or deals that were stopped, modified, or more closely examined as a result of compliance concerns?

- **Funding and Resources** – How have decisions been made about the allocation of personnel and resources for the compliance and relevant control functions in light of the company's risk profile? Have there been times when requests for resources by the compliance and relevant control functions have been denied? If so, how have those decisions been made?

- **Outsourced Compliance Functions** – Has the company outsourced all or parts of its compliance functions to an external firm or consultant? What has been the rationale for doing so? Who has been involved in the decision to outsource? How has that process been managed (including who oversaw and/or liaised with the external firm/consultant)? What access level does the external firm or consultant have to company information? How has the effectiveness of the outsourced process been assessed?

4. Policies and Procedures[3]

a. Design and Accessibility

- **Designing Compliance Policies and Procedures** – What has been the company's process for designing and implementing new policies and procedures? Who has been involved in the design of policies and procedures? Have business units/divisions been consulted prior to rolling them out?

- **Applicable Policies and Procedures** – Has the company had policies and procedures that prohibited the misconduct? How has the company assessed whether these policies and procedures have been effectively implemented? How have the functions that had ownership of these policies and procedures been held accountable for supervisory oversight?

- ☐ **Gatekeepers** – Has there been clear guidance and/or training for the key gatekeepers (*e.g.*, the persons who issue payments or review approvals) in the control processes relevant to the misconduct? What has been the process for them to raise concerns?

- ☐ **Accessibility** – How has the company communicated the policies and procedures relevant to the misconduct to relevant employees and third parties? How has the company evaluated the usefulness of these policies and procedures?

b. **Operational Integration**

- ☐ **Responsibility for Integration** – Who has been responsible for integrating policies and procedures? With whom have they consulted (*e.g.*, officers, business segments)? How have they been rolled out (*e.g.*, do compliance personnel assess whether employees understand the policies)?

- ☐ **Controls** – What controls failed or were absent that would have detected or prevented the misconduct? Are they there now?

- ☐ **Payment Systems** – How was the misconduct in question funded (*e.g.*, purchase orders, employee reimbursements, discounts, petty cash)? What processes could have prevented or detected improper access to these funds? Have those processes been improved?

- ☐ **Approval/Certification Process** – How have those with approval authority or certification responsibilities in the processes relevant to the misconduct known what to look for, and when and how to escalate concerns? What steps have been taken to remedy any failures identified in this process?

- ☐ **Vendor Management** – If vendors had been involved in the misconduct, what was the process for vendor selection and did the vendor in question go through that process? See further questions below under Item 10, "Third Party Management."

5. **Risk Assessment**[4]

- ☐ **Risk Management Process** – What methodology has the company used to identify, analyze, and address the particular risks it faced?

- ☐ **Information Gathering and Analysis** – What information or metrics has the company collected and used to help detect the type of misconduct in question? How has the information or metrics informed the company's compliance program?

- ☐ **Manifested Risks** – How has the company's risk assessment process accounted for manifested risks?

6. Training and Communications[5]

☐ **Risk-Based Training** – What training have employees in relevant control functions received? Has the company provided tailored training for high-risk and control employees that addressed the risks in the area where the misconduct occurred? What analysis has the company undertaken to determine who should be trained and on what subjects?

☐ **Form/Content/Effectiveness of Training** – Has the training been offered in the form and language appropriate for the intended audience? How has the company measured the effectiveness of the training?

☐ **Communications about Misconduct** – What has senior management done to let employees know the company's position on the misconduct that occurred? What communications have there been generally when an employee is terminated for failure to comply with the company's policies, procedures, and controls (*e.g.*, anonymized descriptions of the type of misconduct that leads to discipline)?

☐ **Availability of Guidance** – What resources have been available to employees to provide guidance relating to compliance policies? How has the company assessed whether its employees know when to seek advice and whether they would be willing to do so?

7. Confidential Reporting and Investigation[6]

☐ **Effectiveness of the Reporting Mechanism** – How has the company collected, analyzed, and used information from its reporting mechanisms? How has the company assessed the seriousness of the allegations it received? Has the compliance function had full access to reporting and investigative information?

☐ **Properly Scoped Investigation by Qualified Personnel** – How has the company ensured that the investigations have been properly scoped, and were independent, objective, appropriately conducted, and properly documented?

☐ **Response to Investigations** – Has the company's investigation been used to identify root causes, system vulnerabilities, and accountability lapses, including among supervisory manager and senior executives? What has been the process for responding to investigative findings? How high up in the company do investigative findings go?

8. Incentives and Disciplinary Measures[7]

- **Accountability** – What disciplinary actions did the company take in response to the misconduct and when did they occur? Were managers held accountable for misconduct that occurred under their supervision? Did the company's response consider disciplinary actions for supervisors' failure in oversight? What is the company's record (*e.g.*, number and types of disciplinary actions) on employee discipline relating to the type(s) of conduct at issue? Has the company ever terminated or otherwise disciplined anyone (reduced or eliminated bonuses, issued a warning letter, etc.) for the type of misconduct at issue?

- **Human Resources Process** – Who participated in making disciplinary decisions for the type of misconduct at issue?

- **Consistent Application** – Have the disciplinary actions and incentives been fairly and consistently applied across the organization?

- **Incentive System** – How has the company incentivized compliance and ethical behavior? How has the company considered the potential negative compliance implications of its incentives and rewards? Have there been specific examples of actions taken (*e.g.*, promotions or awards denied) as a result of compliance and ethics considerations?

9. Continuous Improvement, Periodic Testing and Review[8]

- **Internal Audit** – What types of audits would have identified issues relevant to the misconduct? Did those audits occur and what were the findings? What types of relevant audit findings and remediation progress have been reported to management and the board on a regular basis? How have management and the board followed up? How often has internal audit generally conducted assessments in high-risk areas?

- **Control Testing** – Has the company reviewed and audited its compliance program in the area relating to the misconduct, including testing of relevant controls, collection and analysis of compliance data, and interviews of employees and third-parties? How are the results reported and action items tracked? What control testing has the company generally undertaken?

- **Evolving Updates** – How often has the company updated its risk assessments and reviewed its compliance policies, procedures, and practices? What steps has the company taken to determine whether policies/procedures/practices make sense for particular business segments/subsidiaries?

10. Third Party Management [9]

☐ **Risk-Based and Integrated Processes** – How has the company's third-party management process corresponded to the nature and level of the enterprise risk identified by the company? How has this process been integrated into the relevant procurement and vendor management processes?

☐ **Appropriate Controls** – What was the business rationale for the use of the third parties in question? What mechanisms have existed to ensure that the contract terms specifically described the services to be performed, that the payment terms are appropriate, that the described contractual work is performed, and that compensation is commensurate with the services rendered?

☐ **Management of Relationships** – How has the company considered and analyzed the third party's incentive model against compliance risks? How has the company monitored the third parties in question? How has the company trained the relationship managers about what the compliance risks are and how to manage them? How has the company incentivized compliance and ethical behavior by third parties?

☐ **Real Actions and Consequences** – Were red flags identified from the due diligence of the third parties involved in the misconduct and how were they resolved? Has a similar third party been suspended, terminated, or audited as a result of compliance issues? How has the company monitored these actions (*e.g.*, ensuring that the vendor is not used again in case of termination)?

11. Mergers and Acquisitions (M&A) [10]

☐ **Due Diligence Process** – Was the misconduct or the risk of misconduct identified during due diligence? Who conducted the risk review for the acquired/merged entities and how was it done? What has been the M&A due diligence process generally?

☐ **Integration in the M&A Process** – How has the compliance function been integrated into the merger, acquisition, and integration process?

☐ **Process Connecting Due Diligence to Implementation** – What has been the company's process for tracking and remediating misconduct or misconduct risks identified during the due diligence process? What has been the company's process for implementing compliance policies and procedures at new entities?

[1] USSG § 8B2.1(b)(3); FCPA Guide, p.57; USAM 9-28.800 Comment; OECD Handbook, C.1, p.16 *et seq.*

[2] USSG § 8B2.1(2)(B)-(C); FCPA Guide, p.58; USAM 9-28.800 Comment; OECD Handbook, C.3, p. 23 *et seq.*

[3] USSG § 8B2.1(b)(1); FCPA Guide, pp.57-58; OECD Handbook, C.4 and C.5, p.27 *et seq.*

[4] USSG § 8B2.1(b)(5)(7) and (c); USAM 9-28.800 Comment; OECD Handbook, B, p.10 *et seq.*

[5] USSG § 8B2.1(b)(4); FCPA Guide p. 59; USAM 9-28.800 Comment; OECD Handbook, C.8, p. 54 *et seq.*

[6] USSG § 8B2.1(b)(5)(C); FCPA Guide, p. 61; OECD Handbook, C.10, p.60 *et seq.*

[7] USSG § 8B2.1(b)(6); FCPA Guide, pp.59-60; USAM 9-28.800 Comment; OECD Handbook, C.11, p. 68 *et seq.*

[8] USSG § 8B2.1(b)(5)(A)(B); FCPA Guide, pp.61-62; USAM 9-28.800 Comment; OECD Handbook, C.12, pp.72 *et seq.*

[9] FCPA Guide, p.60-66; OECD Handbook, C.6, pp.38 *et seq.*

[10] FCPA Guide, p.62.

Middle Tennessee State University
Audit and Compliance Committee

Tuesday, September 12, 2017 – 10:00am

Tab 6

Green Book to COSO ERM Mapping

Middle Tennessee State University
Board of Trustees

MEETING:	Audit and Compliance Committee
SUBJECT:	*Green Book to COSO ERM Mapping*
DATE:	September 12, 2017
PRESENTER:	Gené Stephens
ACTION:	None

BACKGROUND INFORMATION:

The Committee on Organizations of the Treadway Commission ("COSO") outlined a framework that discusses internal control components for managing enterprise-wide operational and financial risk. In addition, the United States Government Accountability Office (GAO) issued internal control standards and principles in its book, *Standards for Internal Control in the Federal Government*. The GAO's book, known as the "Green Book," aligns with the COSO framework and addresses corporate compliance, risk management, and auditing as tools to help organizations run operations more efficiently and effectively. The Green Book's 17 defined Principles and COSO's five (5) enterprise risk management components additionally coincide with the State of Tennessee's Risk Assessment Toolkit of which MTSU now utilizes to assess all Divisions.

The "Green Book to COSO ERM Mapping" form is provided for the Board's review as background to the State Risk Assessment Forms utilized by the University.

COSO/Green Book IC Components	Green Book Principles[1]	COSO ERM Components	Green Book Attributes	Form #
1. Control Environment	1. The oversight body & management should demonstrate a commitment to integrity and ethical values.	1. Internal Environment	1.02 - 1.10	1
	2. The oversight body should oversee the entity's internal control system.		2.02 - 2.13	
	3. Management should establish an organizational structure, assign responsibility, and delegate authority to achieve the entity's objectives.		3.02 - 3.12[2]	
	4. Management should demonstrate a commitment to attract, develop, and retain competent individuals.		4.02 - 4.08	
	5. Management should evaluate performance and hold individuals accountable for their internal control responsibilities.		5.02 - 5.08	
2. Risk Assessment	6. Management should define objectives clearly to enable the identification of risks and define risk tolerances.	2. Objective Setting	6.02 - 6.07	2
	7. Management should identify, analyze, and respond to risks related to achieving the defined objectives.	3. Event Identification	7.02 - 7.04 8.02 - 8.05 9.02 - 9.03	3
	8. Management should consider the potential for fraud when identifying, analyzing, and responding to risks.	4. Risk Assessment	6.08 - 6.10 7.05 - 7.07 8.06 9.04 - 9.05	
	9. Management should identify, analyze, and respond to significant changes that could impact the internal control system.	5. Risk Response	7.08 - 7.09 8.07	
3. Control Activities	10. Management should design control activities to achieve objectives and respond to risks.	6. Control Activities	10.02 - 10.14	
	11. Management should design the entity's information system and related control activities to achieve objectives and respond to risks.		11.02 - 11.17	
	12. Management should implement control activities through policies.		12.02[3] - 12.05	
4. Information & Communication	13. Management should use quality information to achieve the entity's objectives.	7. Information & Communication	13.02 - 13.06	4
	14. Management should internally communicate the necessary quality information to achieve the entity's objectives.		14.02 - 14.08	
	15. Management should externally communicate the necessary quality information to achieve the entity's objectives.		15.02 - 15.09	
5. Monitoring	16. Management should establish and operate monitoring activities to monitor the internal control system and evaluate the results.	8. Monitoring	16.02 - 16.10[4]	5
	17. Management should remediate identified internal control deficiencies on a timely basis.		17.02 - 17.06[5]	

Minimum Documentation Requirements

[1] Paragraph OV2.06 - If management determines that a principle is not relevant, management supports that determination with documentation that includes the rationale of how, in the absence of that principle, the associated component could be designed, implemented, and operated effectively.

[2] Paragraph 3.09 - Management develops and maintains documentation of its internal control system.

[3] Paragraph 12.02 - Management documents in policies the internal control responsibilities of the organization.

[4] Paragraph 16.09 - Management evaluates and documents the results of ongoing monitoring and separate evaluations to identify internal control issues.

[5] Paragraph 17.05 - Management evaluates and documents internal control issues and determines appropriate corrective actions for internal control deficiencies on a timely basis.

Middle Tennessee State University
Audit and Compliance Committee

Tuesday, September 12, 2017 – 10:00am

Tab 7

Compliance and ERM Overview and Activities

Middle Tennessee State University
Board of Trustees

MEETING:	Audit and Compliance Committee
SUBJECT:	*Compliance and ERM Overview and Activities*
DATE:	September 12, 2017
PRESENTER:	Gené Stephens
ACTION:	None

BACKGROUND INFORMATION:

The Office of Compliance and Enterprise Risk Management (CAREM or Office) is a new office within the Division of Business and Finance that began on January 3, 2017. The Office is responsible for identifying, assessing, and monitoring institutional and enterprise-wide risks and compliance activities in support of the University's mission, academic programs, and operations. CAREM additionally provides support to all University Divisions regarding compliance training and tools; risk mitigation strategies; and regulatory updates on higher education topics. The Office additionally facilitates the MTSU Enterprise Compliance & Risk Management Committee that will serve as the University's internal Corporate Compliance Committee (Committee). The Committee will include faculty from both the undergraduate and graduate colleges, as well as representatives from key divisions/units.

The "Compliance and ERM Overview and Activities" document discusses the Office's Statement of Purpose and activities for the Board's review and comment. Additional information about the Office can be found on the following webpage at www.mtsu.edu/carem.

Middle Tennessee State University
Office of Compliance and Enterprise Risk Management

Statement of Purpose

- To promote an ethical culture of integrity and accountability in support of MTSU's mission, operations, and strategic goals.

- To enhance the University's enterprise-wide compliance risk management activities by:

    1. Creation of additional risk assessment tools (risk dashboard and enterprise-wide regulatory calendar).

    2. Development of an Enterprise Compliance and Risk Management Committee (corporate compliance committee).

    3. Development of a Corporate Compliance Plan.

    4. Development of a Risk Management Operations Manual.

- To prevent fraud, waste, and abuse through appropriate corporate compliance planning and risk management activities in compliance with State requirements and SACSCOC Principles.

- To provide educational training opportunities and resources regarding higher education compliance, ethics, and risk management best practices.

- To mitigate conflict of interests, ethics violations, and inadequate risk controls through regular and systematic risk assessments.

- To serve as a thought partner and collaborator on risk management issues and corporate compliance challenges.

- To provide consultation and support related to risk management and compliance of auxiliary business areas (insurance, contracts, safety).

Risk Management Activities

1. Department webpage creation – www.mtsu.edu/carem.

2. Development of a Conflict of Interest Checklist for Faculty (to be reviewed by Faculty Senate, the Chairs Council, and the Dean's Council).

3. Development of four (4) training presentations:

    a. Privacy and Confidentiality
    b. Ethics
    c. Fraud, Waste, and Abuse
    d. HIPAA

4. Risk Dashboard creation (in process in collaboration with MTSU ITD).

5. Risk Management Operations Manual

6. Executive Risk Assessment Report

7. Development of Executive Risk Assessment Heat Map.

8. Current development of a regulatory reporting database for the entire enterprise.

State Risk Assessment Reporting

1. Deadline for submission of risk assessments to the State – September 29, 2017.

2. Process:

    a. Specified MTSU Divisions complete risk assessments every three years. For 2017, the President's Office and ITD's risk assessments will be submitted to the State.

    b. MTSU Utilizes the State's Optional ERM Toolkit, which is modeled after the COSO Green Book ERM Principles.

    c. The State's Optional ERM Toolkit was introduced to all institutions in January 2017.

Corporate Compliance Activities

1. Enterprise Compliance and Risk Management Committee

    a. To meet twice annually (October and March).
    b. Will include faculty representation (graduate and undergraduate colleges) for shared governance.
    c. Supports the progress and continued success of MTSU by:
        i. Considering innovative solutions to workplace risks and risk controls;
        ii. Recommending programming to promote MTSU's community standards;
        iii. Reviewing employee training regarding operational and regulatory topics to determine if improvements are needed;
        iv. Developing a long-range strategic plan to promote diversity and civility among faculty, staff, and students.

2. Development of Compliance Plan in collaboration with the Enterprise Compliance and Risk Management Committee

3. Annual Compliance Week Activities (Compliance week is November 5-11 , annually)

4. Oversight of Records Management (retention, destruction, and maintenance of records)

Middle Tennessee State University
Audit and Compliance Committee

Tuesday, September 12, 2017 – 10:00am

Tab 8

Financial Integrity Act and State Risk Assessment Reporting

Middle Tennessee State University
Board of Trustees

MEETING:	Audit and Compliance Committee
SUBJECT:	*Financial Integrity Act and State Risk Assessment Reporting*
DATE:	September 12, 2017
PRESENTER:	Gené Stephens
ACTION:	None

BACKGROUND INFORMATION:

The Financial Integrity Act ("the Act"), codified in Tennessee Code Annotated ("TCA") § 9-18-102(3)(b), requires state agencies and institutions of higher education to annually perform a management assessment of risk and to incorporate internal risk controls in the assessment (attached). The risk management assessments must also provide reasonable assurances that the institution is: "(1) accountable for meeting program objectives; (2) promoting operational efficiency and effectiveness; (3) improving reliability of financial statements; (4) strengthening compliance with laws, regulations, rules, contracts, and grant agreements; and (5) reducing the risk of financial, or other asset losses, due to fraud, waste, and abuse."

Section 9-18-104 of the Act (attached) requires state agencies and institutions of higher education to prepare and provide a management assessment of risk to the State of Tennessee's Commissioner of Finance and Administration and to the Comptroller of the Treasury by December 31 annually. The annual report must also contain an acknowledgment of the institution's management responsibilities for establishing, implementing, and maintaining an adequate system of internal control together with the risk assessment report that documents objectives, risk mitigation activities, and an action plan to correct weaknesses.

The Divisions scheduled to submit risk assessment documentation utilizing the State of Tennessee's new Risk Management Toolkit are the Information Technology Division (ITD) and the President's Office. In addition, each University Division has an assigned Risk Assessment Coordinator to assist with the compilation and completion of the risk assessment forms.

Tenn. Code Ann. § 9-18-102

*** Current through the 2016 Regular Session and the 2nd Extraordinary Session of the 109th Tennessee General Assembly ***

Title 9 Public Finances
Chapter 18 Financial Integrity Act of 1983

Tenn. Code Ann. § 9-18-102 (2016)

9-18-102. Internal controls -- Management assessment of risk.

(a) Each agency of state government and institution of higher education along with each county, municipal, and metropolitan government shall establish and maintain internal controls, which shall provide reasonable assurance that:

(1) Obligations and costs are in compliance with applicable law;

(2) Funds, property, and other assets are safeguarded against waste, loss, unauthorized use, or misappropriation; and

(3) Revenues and expenditures are properly recorded and accounted for to permit the preparation of accurate and reliable financial and statistical reports and to maintain accountability over the assets.

(b) To document compliance with the requirements set forth in subsection (a), each agency of state government and institution of higher education shall annually perform a management assessment of risk. The internal controls discussed in subsection (a) should be incorporated into this assessment. The objectives of the annual risk assessment are to provide reasonable assurance of the following:

(1) Accountability for meeting program objectives;

(2) Promoting operational efficiency and effectiveness;

(3) Improving reliability of financial statements;

(4) Strengthening compliance with laws, regulations, rules, and contracts and grant agreements; and

(5) Reducing the risk of financial or other asset losses due to fraud, waste and abuse.

HISTORY: Acts 1983, ch. 129, § 1; 1998, ch. 664, §§ 1, 2; 2008, ch. 750, § 1; 2015, ch. 112, § 1.

Tenn. Code Ann. § 9-18-104

*** Current through the 2016 Session ***

Title 9 Public Finances
Chapter 18 Financial Integrity Act of 1983

Tenn. Code Ann. § 9-18-104 (2016)

9-18-104. Report by head of executive agency.

(a) By December 31, 2008, initially, and then by December 31 of every year thereafter, the head of each state agency and higher education institution shall, on the basis of the evaluations conducted in accordance with guidelines prescribed under § 9-18-103, prepare and transmit to the commissioner of finance and administration and the comptroller of the treasury a report that states that:

(1) The agency or institution acknowledges its management's responsibility for establishing, implementing and maintaining an adequate system of internal control; and

(2) A management assessment of risk performed by the agency or institution provides or does not provide reasonable assurance of compliance with the objectives of the assessment as specified in this chapter.

(b) In the event that the agency's or institution's assessment does not provide reasonable assurance of compliance with the objectives of the assessment as stated in this chapter, the report shall include a corrective action plan that identifies:

(1) Any significant deficiencies or material weaknesses in the agency's or institution's system of internal control and/or lack of risk mitigating control activity; and

(2) The plans and the schedule for correcting the weaknesses.

HISTORY: Acts 1983, ch. 129, § 1; 1998, ch. 664, §§ 4-6; 2008, ch. 750, § 3; 2009, ch. 99, § 1.

Middle Tennessee State University
Audit and Compliance Committee

Tuesday, September 12, 2017 – 10:00am

Tab 9

Risk Assessment Report Submittal

Middle Tennessee State University
Board of Trustees

MEETING:	Audit and Compliance Committee
SUBJECT:	*Risk Assessment Reporting Submittal*
DATE:	September 12, 2017
PRESENTER:	Gené Stephens
ACTION:	Voice Vote
STAFF RECOMMENDATION	Approval

BACKGROUND INFORMATION:

Section 9-18-104 of the Financial Integrity Act requires institutions of higher education to prepare and provide a management assessment of risk to the State of Tennessee's Commissioner of Finance and Administration and to the Comptroller of the Treasury by December 31 annually.

The results of the risk assessment for the Information Technology Division and President's Office were designated as confidential and discussed in the non-public Executive session of the Audit and Compliance Committee. The Audit and Compliance Committee is responsible for the oversight and monitoring of internal controls, compliance, and risk management functions of the University; therefore, the risk assessment reports are presented to the Committee for approval prior to the reports submission to the State, as required by law.