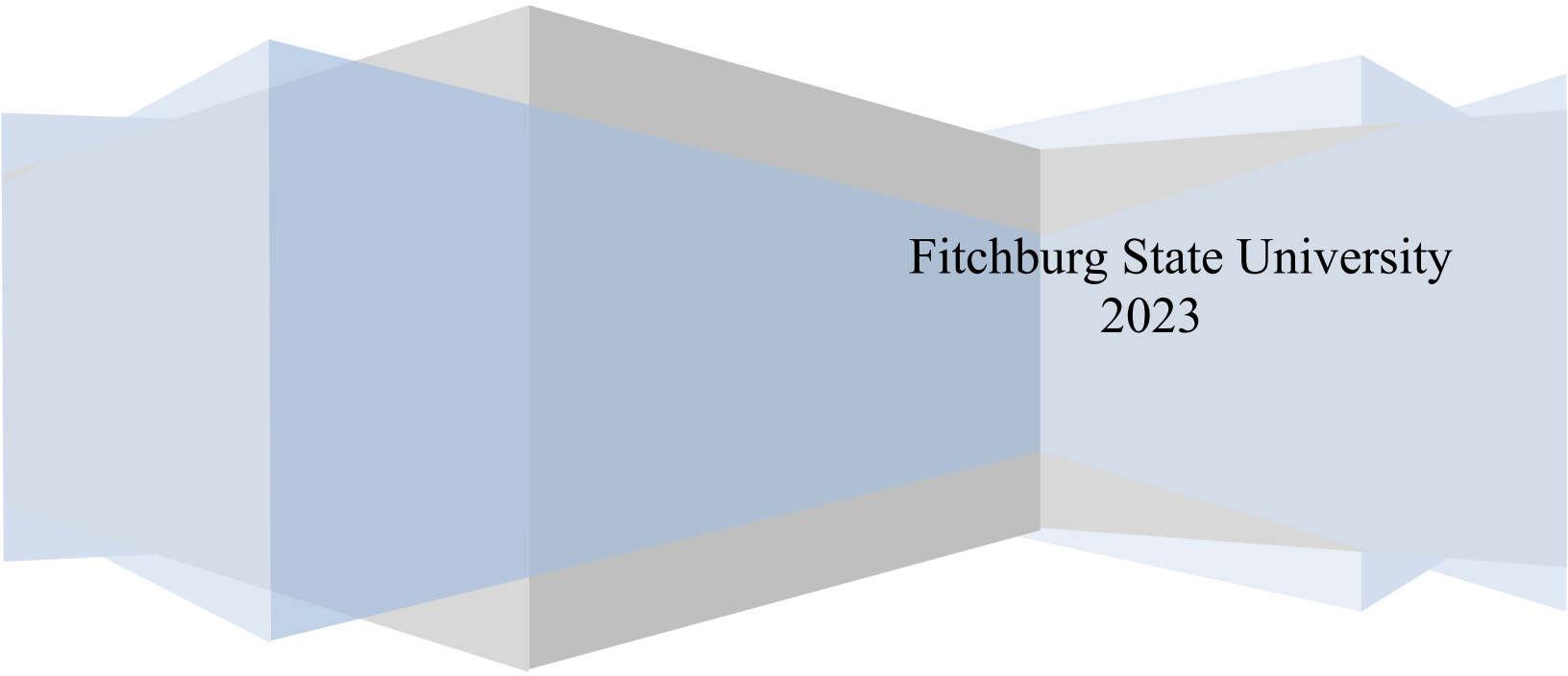
Internal Control Plan



Fitchburg State University
2023

FITCHBURG STATE UNIVERSITY
INTERNAL CONTROL PLAN

To the University Community

Chapter 647 of the Acts of 1989, *An Act Relative to Improving Internal Controls Within State Agencies,* establishes the minimum level of quality acceptable for the internal control systems in operation throughout state departments, agencies and universities. The Office of the State Auditor and the Office of the State Comptroller are legislatively mandated to enforce the state law. Internal Control Plans (ICP) are based on comprehensive assessment of risk, especially those related to the prevention of fraud, waste and abuse. An effective ICP requires the involvement of everyone in the organization. Department heads and managers must develop internal controls for each activity for which they are responsible. The internal controls exercised over individual activities, when taken collectively, become the internal controls of the program or administrative function of which they are part. The internal controls for each department's programs and administrative functions, when combined with overall department controls, comprise the University's internal control documentation. This documentation, or high-level overview describing, referencing, and summarizing the documentation, is the University's *Internal Control Plan.*

Management's role is to provide the leadership that the University needs to achieve its goals and objectives. Internal controls are the structures, policies and procedures used to ensure that management accomplishes its objectives and meets its responsibilities effectively and efficiently while at the same time assuring compliance with applicable rules, regulations and laws. Thus it is imperative that the Internal Control Plan be reviewed and updated. Each manager is responsible for reviewing and updating his/her section of the Internal Control Plan at least on an annual basis and as conditions warrant.

Any questions or comments may be directed to the University's Internal Control Officer, Jay Bry, Vice President of Finance and Administration.

Sincerely,

Richard S. Lapidus
President

Overview of Internal Controls

Introduction

Chapter 647 of the Acts of 1989, *An Act Relative to Improving Internal Controls Within State Agencies*, establishes the minimum level of quality acceptable for Internal Control Systems in operation throughout state departments, agencies and universities. The Office of the State Auditor and the Office of the State Comptroller are legislatively mandated to enforce this state law.

This guide is based on the Committee of Sponsoring Organizations (COSO) *Enterprise Risk Management Framework* (ERM) and it also includes the Federal Government's standard of Internal Control, the Green Book, which is an adaptation of COSO's internal control – Integrated Framework (2013).

COSO defines internal control as follows:

"Internal control is a process, effected by an entity's board of directors, management and other personnel, designed to provide reasonable assurance regarding the achievement of goals and objectives in the following categories:

- Operations - Effectiveness and efficiency of operations.
- Reporting - Reliability of internal and external financial and non-financial reporting.
- Compliance - Compliance with applicable laws and regulations.

This definition reflects certain fundamental concepts:

- Internal control is a process. It is a means to an end, not an end itself.
- Internal control is affected by people. It is not policy manuals and forms, but people at every level of an organization.
- Internal control can be expected to provide only reasonable assurance, not absolute assurance, to an entity's management and board.
- Internal control is geared to the achievement of objectives in one or more separate but overlapping categories.
- Internal control is adaptable to the entire university – flexible in application for the university or for a particular department or business process.

Internal controls are based on comprehensive assessments of risks and require the involvement of everyone within an organization. A less technical definition might state that:

> Internal controls are tools that help managers be effective and efficient while avoiding serious problems such as overspending, operational failures, and violations of law.

Components of Internal Controls

Per the COSO ERM framework, there are eight interrelated components to internal control. They are as follows:

1. **Internal Environment** – The foundation for all other components of internal control and includes the organization's culture, philosophy and ethical values. The organization structure, authority, responsibility and accountability are necessary to plan, execute, control and assess the achievement of its objective.

2. **Objective Setting** – Objective setting is required to achieve the strategic goals of an organization and can be either short or long term in nature. A good objective is SMART: specific, measurable, attainable, results-focused and timely. Once the objectives are established, the organization should then determine its risk appetite (amount of risk the organization is willing to accept to achieve its objectives) and its risk tolerance (the acceptable deviation from the organization risks).

3. **Event Identification** – The process by which an organization identifies events that might have an impact on the organization's ability to achieve its objectives both internally and externally. It includes distinguishing between events that represent risks, those that represent opportunities, and those that may be both.

4. **Risk Assessment** – Identified risks are analyzed in order to form a basis for determining how they should be managed. Risks are associated with objectives that may be affected. Risks are assessed on both inherent and residual basis, with the assessment considering both the risk likelihood and impact. Risk assessment needs to be done continuously and throughout the university.

5. **Risk Response** – The organization's plan to manage identified risks within its defined levels of risk tolerance and risk appetite.

6. **Control Activities** – The structures, policies, and procedures that the organization establishes to identify and respond to risks that could prevent it from achieving its goals and objectives.

7. **Information and Communication** – Data generated from both internal and external sources is used to provide information to manage risks and make decisions. Effective communication occurs multi-dimensionally flowing up, down and across the organization and to external stakeholders.

8. **Monitoring** – An organization's continued efforts to monitor the effectiveness of its controls. Proper monitoring ensures that controls continue to be adequate and continue to function properly and that any deficiencies are promptly reported to and corrected by management.

FITCHBURG STATE UNIVERSITY

Internal Control Plan

Internal Environment

Fitchburg State University (FSU) was chartered in 1894 to provide residents of the state with quality and affordable degrees; it operates under the enabling legislation found in the Massachusetts General Laws, Chapter 73, as amended.

FSU's mission statement was approved by the Board of Trustees in 2010, and it aligns with the MA Board of Higher Education Mission Statement and the MA Department of Higher Education's mission for the State Universities. It reads: "Fitchburg State University is committed to excellence in teaching and learning and blends liberal arts and sciences and professional programs within a small college environment. Our comprehensive public university prepares students to lead, serve and succeed by fostering lifelong learning and civic and global responsibility. A Fitchburg State education extends beyond our classrooms to include residential, professional, and co-curricular opportunities. As a community resource, we provide leadership and support for the economic, environmental, social and cultural needs of North Central Massachusetts and the Commonwealth."

Per Massachusetts General Laws, Chapter 15A, as amended, the Board of Higher Education (BHE) is the official governing organization of each of the universities in Massachusetts. Fitchburg State University is governed directly by an eleven-member Board of Trustees (BOT). Nine are appointed by the governor for a five-year term, one alumni trustee is elected by the alumni association for a five-year term, and a student trustee is elected by the student body for one year. The BOT meets four times annually or as needed and works through its committees: Executive, Academic Affairs, Administration and Finance, Personnel, Student Life, which meet on an as-needed basis. BHE is responsible for setting tuition and approving academic programs and admission standards, mission statements, strategic plans, presidential appointments, and annual budgets and spending plans, while the BOT oversees the local governance of FSU by establishing all fees; making policies for the administrative management of personal and the general business of the institution; review financial statements and federal tax reports, and overseeing the budget process, annual self-assessments, and five-year plans. The Board communicates with the University community not only through the President of the University, but also through the administrative liaisons assigned to the Board committees.

The University strives to be fully compliant with all local, state and federal laws, rules and regulations governing its various operations, and, adheres both to the "letter" of each law, rule or regulation, as well as, to its original intent and "spirit." In compliance with applicable laws, rules and regulations, FSU through its organizational structure, standing committees, affirmative action/equal opportunity policies, its three collective bargaining agreements, its academic and student life policies and procedures, and its administrative and financial policies and procedures has developed an environment that encompasses both technical competence and ethical commitment. The University is committed to hire, train, and retain qualified competent staff.

Faculty and staff in leadership roles are responsible for the application of this policy and the design, development, implementation, and maintenance of an effective and efficient system of internal

controls within their respective areas of responsibility. Subject matter experts (SME) are identified across the university and specifically in high-risk areas including, but not limited to, Accounts Payable, Budget, Finance, Procurement Services, Human Resources, and Information Technology. SMEs are required to:

- Develop, implement, and review internal controls policy and training in their area of expertise.
- Perform internal control reviews on an ongoing basis.
- Promote the internal control program within their area of expertise to gain consistency in the way the university thinks about risk.
- Encourage a culture that self-identifies gaps in internal controls and aids in mitigation of the identified risk.

Objective Setting

The purpose of the Fitchburg State University Internal Control Plan is to provide the Board of Trustees and other outside federal and state agencies with reasonable assurance that the University is efficiently and effectively meeting in a cost-effective manner the goals and objectives outlined in the strategic plan and mission of the University.

The Internal Control Plan further strives to identify and summarize university-wide risks and the controls in place to mitigate those risks, (risk appetite versus risk tolerance). University-wide risks are delineated in the four categories below:

- <u>The safeguarding of all assets (financial and non-financial):</u>

Assets and records must be kept secure at all times to prevent unauthorized access, loss or damage. Assets such as cash, equipment, inventory, financial, software, sensitive personal information, and management policy and procedures to reasonably ensure resources are protected against misuse or loss. The security of assets and records is essential for accurate and ongoing operations.

- <u>Ensure the validity and reliability of all data:</u>

The university should implement and apply reasonable control procedures to ensure that valid, timely and reliable data are obtained, maintained and fairly disclosed in reports. This includes both financial and non-financial data. If the data is inaccurate, incomplete or misleading, the reported operations cannot function properly, and this may mislead not only management but students, creditors and donors.

- <u>Ensure compliance with applicable laws and regulations:</u>

The university should implement policies and procedures in order to ensure that all department activities and the acquisition and use of resources comply with local, federal, and state laws and regulations.

- <u>Ensure alignment of goals throughout the university:</u>

Aligning goals is an important part of a successful operation. Strategic alignment is the process of planning and implementing practices to ensure an organization's strategies support its general objectives. In a strategically-aligned organization, all departments, decisions and functions contribute to the fulfillment of the organization's mission, vision and objectives. Employees thus informed of how their department objective adds value to the university's overall strategy may use their time more efficiently to make informed decisions about which tasks best serve the university's goals and focus their efforts accordingly.

All departments should have clear articulated objectives and management along with their staff should at least yearly review these goals/objectives to ensure that they are aligned with the current strategic plan of the University and with internal and external expectations. Management should foster a climate that encourages employees' knowledge of and compliance with all the university policies and procedures, especially those that are in the employee purview.

Event Identification

The University, through its strategic, budgetary planning and daily exercises, identifies events that could potentially affect its ability to fulfill the mission of the University. Events with negative impact represent risks that need to be addressed by management- e.g. COVID. Events with positive impact represent opportunities that could be incorporated into strategic planning and objective modeling-e.g. COVID. The event risk can be broadly categorized into the following four types:

- Opportunity risk – Refers to the possibility of losing a viable opportunity while pursuing different available options.
- Risk of Uncertainty – Risk of uncertain events happening that could affect the smooth operations of the university.
- Risk of Hazards – Risk of a dangerous event happening that could arise out of a poor workplace design or improper allocation of duties depending on one's skill set.
- Operational Risk – Risk associated with day-to-day business activities. Risk occurs because of the failure of processes, policies or systems.

Identified risks can be inherent and/or residual. Inherent risk is the possibility that an event will occur and adversely affect the University (mistake, omission, or error). Residual risk is what remains after management responds to inherent risk. When identifying risk, it is particularly important to consider the potential for fraud, waste and abuse.

Fraud risk factors do not necessarily indicate that fraud exists but are often present when fraud occurs. Fraud risk factors include the following:

- Incentive/pressure - Management or other personnel have an incentive or are under pressure to meet a deadline or performance target, which provides a motive to commit fraud.
- Opportunity - Circumstances exist, such as the absence of controls, ineffective controls, or the ability of management to override controls, that provide an opportunity to commit fraud.

- Attitude/rationalization - Individuals involved are able to rationalize committing fraud. Some individuals possess an attitude, character, or ethical values that allow them to knowingly and intentionally commit a dishonest act

(See Fitchburg State University's Preventing and Reporting Fraud, Waste and Abuse Policy for further details.)

Risk Assessment

Risk assessment is the process used to identify, classify, analyze and manage the risks that could prevent the University from attaining its goals and objectives. Changes in conditions affecting the university and its environment often require changes to the university's internal control system, as existing controls may not be effective for meeting objectives or addressing risks under changed conditions – e.g. internet security risks.

Management analyzes the effect of identified changes on the internal control system and responds by revising the internal control system on a timely basis, when necessary, to maintain its effectiveness. Changing conditions often prompt new risks or changes to existing risks that need to be assessed.

Fitchburg State University uses a variety of tools to assess risk including evaluation of systems, questionnaires and periodic internal and external reviews. The University requires departments to annually review the department's objective and the key components to achieving those objectives and then do a risk assessment. After doing a risk assessment, the department should:

- Do a short summary and state how and when the risk assessment was conducted.
- The persons involved in doing the risk assessment
- How the risks were rated (what was the scale/methodology used and was it used applied consistently throughout the process),

Once risks have been identified, they are prioritized based on the likelihood of occurrence and the severity of the consequence as follows:

- Level I requires immediate action and senior management involvement
- Level II requires management responsibility and action to be specifically assigned
- Level III can be managed by specific response and monitoring
- Level IV can be managed by routine process

  Grouping the departmental risks in these categories permits the analysis of the adequacy of existing controls, the identification of any patterns of risks and whether any concentration of risks exist in a particular area.

Risk Response

Risk management includes both risk assessment and the process of addressing risks (control activities) that are identified from the assessment. There are four basic management approaches to dealing with identified risks. They are as follows:

1. Accept the risk
2. Avoid the risk
3. Share the risk with third parties (i.e. insurers)
4. Mitigate the risk by designing processes that eliminate or reduce the risk

Due to the cost/benefit relationship, it is not possible to mitigate every risk that could potentially affect an organization. It should also be noted that some residual risk will remain even after efforts have been made to address identified risk. In addition, if the risk is not critical, management may be willing to accept a certain level of risk to achieve its goals and objectives.

Control Activities

Control activities consist of policies and procedures established by management to achieve objectives and respond to risks identified in the Internal Control Plan. Control activities can be designed at the entry level and/or the transaction level depending on the precision needed for the department to meet its objective.

Managers must develop policy and procedures for each activity for which they are responsible. The internal controls exercised over individual activities, when taken collectively, become the internal controls of the program or administrative function of which they are a part. The internal controls for each of a department's programs and administrative functions, when combined with overall department controls, comprise the University's internal control documentation.

This documentation is required by Chapter 647 of the Acts of 1989. The University's Internal Control Plan is a high-level overview describing, referencing and summarizing all the individual department documentation.

Types of Internal Control and Common Control Activities

A system of internal control can be evaluated by assessing its ability to achieve seven commonly accepted control objectives:

- **Segregation of Duties** – To prevent the occurrence of undetected errors or fraud, responsibilities must be divided so that one individual does not control all aspects of a transaction.
- **Safeguarding Assets** – Assets (including cash) and records must be kept secure at all times to prevent unauthorized access, loss or damage. The security of assets and records is essential for accurate operations.

- **Safeguarding Confidential Information** – Ensure the security and confidentiality of personal and private information, protect against any anticipated threats to its security or integrity, and guard against unauthorized access and use.
- **Review and Approval** – Review and approval of internal processes should be obtained from a knowledgeable and independent party to ensure that transactions have been executed in accordance with management's general authorization.
- **Timeliness** – Make all efforts to meet prescribed deadlines and prioritize critical work to avoid fines and negative impacts on operational processes.
- **Error Handling** – Errors detected at any stage of processing receive prompt corrective action and are reported to the appropriate level of management.
- **Documentation** – Provide evidence for transactions to support accuracy and consistency.

Preventive and Detective are two major types of controls.

Preventative controls - Designed to forestall errors or irregularities and thereby avoid the cost of corrections. Examples of common preventive control activities include:

- Segregation of duties
- Proper authorization to prevent improper use of organizational resources
- Standardized forms
- Physical control over assets
- Computer passwords
- Computerized techniques such as transaction limits and system edits

Detective controls - Designed to measure the effectiveness of preventive controls and detect errors or irregularities when they occur. These controls are less effective and more expensive than preventive controls because they occur at the back end of the process. Examples of common detective control activities include:

- Performance and quality assurance reviews
- Reconciliations
- Cash counts
- Physical inventory counts and comparisons with inventory records

Information & Communication

Fitchburg State University posts its Internal Control Plan, as well as many other policy documents on its web page. In addition, newsletters and informative memoranda from key departments are routinely distributed to the University community. There are scheduled and unscheduled meetings ranging from the President's cabinet meeting to various committee, departmental and neighborhood meetings. These are all an effort to provide various forums for the exchange of information and ideas and to foster communication and cooperation.

Management must ensure that employees are aware of the internal control policies of the department.

Monitoring

Monitoring University operations occurs on an ongoing basis through the normal course of management activities. New initiatives are evaluated for both the strength of the opportunity or associated risk they may present. Fitchburg State University reviews and updates the Internal Control Plan on a regular basis as needed. The University's external accounting firm, as part of its audit procedures, reviews the University's internal controls in accordance with current auditing standards and legislative requirements.

Internal Control Plan Review

Reviewed/NCN _____ Date _____

Reviewed/NCN _____ Date _____

Reviewed/NCN _____ Date _____

Reviewed/NCN _____ Date _____

Reviewed/NCN _____ Date _____