

University of Wisconsin-Extension

INTERNAL CONTROL PLAN



TABLE OF CONTENTS

| | |
|---|-----------|
| TABLE OF CONTENTS _____ | 1 |
| Introduction _____ | 3 |
| UW-Extension Select Mission _____ | 3 |
| Governance _____ | 4 |
| Organizational Structure _____ | 4 |
| Board of Regents _____ | 4 |
| Chancellor _____ | 4 |
| Chief Business Officer (CBO) and Chief Financial Officer (CFO) _____ | 5 |
| Controller _____ | 5 |
| Internal Audit _____ | 6 |
| Financial Statements and Other Audited Reports _____ | 6 |
| Code of Conduct _____ | 7 |
| Internal Control: Overview _____ | 7 |
| Control Environment _____ | 9 |
| Risk Assessment _____ | 9 |
| Business _____ | 10 |
| Financial _____ | 10 |
| Operational _____ | 10 |
| Information Technology _____ | 10 |
| Public and Political Sensitivity _____ | 10 |
| Compliance Requirements _____ | 10 |
| Information and Reporting _____ | 10 |
| Organization Change and Growth _____ | 10 |
| Consideration of Internal Control Over Key Subcycles _____ | 10 |
| Control Activities _____ | 11 |
| Monitoring _____ | 12 |
| Information and Communication _____ | 13 |
| UW-System Administration (UWSA) _____ | 14 |
| Business Services _____ | 14 |
| Internal Audit _____ | 15 |
| Statement of Support for Internal Accounting Control _____ | 16 |
| Annex A - UW-Extension Executive Level Organization Chart _____ | 17 |
| Annex B - UW-Extension Admin & Fin Srvs Organization Chart _____ | 18 |
| Annex C – UW-Extension Charter _____ | 19 |
| Annex D - Financial Statements for FY 2007 _____ | 21 |
| Annex E - Internal Control Matrices _____ | 24 |
| E-1 Control Matrix – Revenues _____ | 24 |
| E-2 Control Matrix – Disbursements Nonpayroll _____ | 26 |

**The University of Wisconsin – Extension
Internal Control Plan – March 2009**

| | |
|--|----|
| E-3 Control Matrix – General Ledger Entries _____ | 30 |
| E-4 Control Matrix – Purchasing Card (P-Card) _____ | 32 |
| E-5 Control Matrix – Cash Handling (Cash, Check, Money Order, Traveler’s Check, Credit Card) _____ | 36 |
| E-6 Control Matrix – Capital Assets _____ | 41 |
| E-7 Control Matrix – Fraud Detection _____ | 44 |
| E-8 Control Matrix – Human Resources – Hiring Practices _____ | 51 |
| E-9 Control Matrix – Human Resources – Employment/Payroll Practices _____ | 55 |
| E-10 Control Matrix – Information Technology – General Controls _____ | 62 |
| E-11 Control Matrix – Information Technology – Application Controls _____ | 69 |
| E-12 Control Matrix – Payment Card Data Security Controls (Processed/Stored by UWEX) _____ | 71 |
| E-13 Control Matrix – Payment Card Data Security Controls (Processed/Stored by Vendor) _____ | 76 |

Introduction

This Internal Control Plan is prepared in accordance with the delegation agreement signed between the State Controller and the University of Wisconsin System Administration (UWSA) entitled “Cooperative Agreement on Accounting, Auditing, and Internal Control Activities.” For the most part, the processing of University of Wisconsin-Extension (UW-Extension) financial transactions takes place at UW-Extension and most of the relevant controls are exercised at that level. Thus, this plan is an extension of the delegation from the Department of Administration to the UW System as authorized by section 16.53 of the Wisconsin Statutes and the delegation agreement existing between the UWSA and UW-Extension.

Every organization, be it governmental, for profit, or not-for-profit, exists to achieve some purpose or goal. UW-Extension’s goals are outlined in its Mission Statement, which is included below. It is the role of management to provide the leadership needed for the UW-Extension to achieve its goals and objectives. Internal control is a coordinated set of policies and procedures for achieving management objectives.

UW-Extension Select Mission

Through the UW-Extension, all Wisconsin people can access university resources and engage in lifelong learning, wherever they live and work.

Fundamental to this mission are UW-Extension's partnerships with the 26 UW campuses, the county and tribal governments, and other public and private organizations. Fulfilling the promise of the Wisconsin Idea, UW-Extension extends the boundaries of the university to the boundaries of the state and helps the university establish mutually beneficial connections with all its stakeholders.

For millions of Wisconsin individuals, families, businesses and communities, UW-Extension is the doorway to their public university, enabling them to:

- Achieve personal growth, professional success and organizational effectiveness through formal and informal learning;
- Address the changing needs of the state and society by applying relevant university research; and
- Gain greater access to educational, cultural and civic resources through the use of technologies.

In addition, UW-Extension supports the University of Wisconsin System mission by:

- Providing strong leadership for the university's statewide public service mission;
- Integrating a scholarly approach to outreach across many academic disciplines; and
- Addressing the specific educational needs of under-served, disadvantaged and non-traditional students.

The mission of the UW-Extension includes the programs of the four UW-Extension programmatic divisions: Cooperative Extension; Continuing Education, Outreach and E-Learning Extension; Broadcasting & Media Innovations, and Entrepreneurship and Economic Development.

Governance

As provided in Chapter 36 of the Wisconsin Statutes, primary responsibility for the governance of the system is vested in the Board of Regents which is responsible for establishing policies and rules for governing the system, planning to meet future state needs for collegiate education, setting admission standards and policies, reviewing and approving university budgets and establishing the regulatory framework within which the individual units are allowed to operate with as great a degree of autonomy as possible.

Organizational Structure

Board of Regents

The Board of Regents appoints the president of the system, the chancellors of the 13 universities, UW-Extension and UW College and the deans who head each of the 13 colleges. The President and Chancellors are charged with implementing regent policies and with administration of the institutions. System Administration is responsible to the president and assists the Board of Regents in establishing policies, reviewing the administration of policies and planning the programmatic, financial and physical development of the system.

Chancellor

The Chancellor of UW-Extension is the executive head of the institution, responsible for the administration of the institution including auxiliary services and budget management. Faculty, academic staff and students share in the governance of the institutions as provided by law subject to the responsibilities and powers of the board, the President and Chancellors.

The Chancellor is served by a Vice Chancellor/Provost, an Associate Vice Chancellor, a Senior Special Assistant, and a Senior Administrative Program Specialist. Directors of University Relations, Government Relations, Diversity/Workforce Development, Human Resources, Information Technology also serve the Chancellor. A Dean of Continuing Education, Outreach and E-Learning, a Dean for Cooperative Extension, a Director for Broadcasting and Media Innovations and a Director of Entrepreneurship and Economic Development also serve the Chancellor. Each of these individuals is responsible for formulating, interpreting and implementing policies within his/her assigned divisions and area of responsibility.

See Annex A for an executive level UW-Extension organization chart.

Chief Business Officer (CBO) and Chief Financial Officer (CFO)

Responsibility for the major business functions of the UW-Extension is assigned to the Associate Vice Chancellor for Administrative and Financial Services, who serves as UW-Extension's CBO and CFO. The Associate Vice Chancellor for Administrative and Financial Services serves as the liaison to UW College, other divisions, other UW-System institutions, State and local governments, and other State agencies. The Budget Director, Controller, Conference Center Director, Internal Auditor, Facilities, Mail Services and Risk Management Director report directly to the Associate Vice Chancellor.

An organization chart for the Administrative and Financial Services (AFS) is provided in Annex B.

Controller

The UW-Extension Controller is the Director of Business Services. Business Services, a department within AFS, is committed to provide a variety of business and financial services to support the UW-Extension community while ensuring proper internal control in accordance with UW System, State and Federal requirements. The Controller is charged with the responsibility to define, document, implement and communicate fiscal policy, account for financial resources and to issue financial reports.

The Controller directs and is responsible for UW-Extension accounting practices, maintenance of fiscal records and preparation of institutional financial reports. This includes assuring that accounting activities are in compliance with Generally Accepted Accounting Principles and with University of Wisconsin System and State of Wisconsin laws, rules and regulations. The Controller is responsible for developing policies and procedures that provide a strong system of internal control to assure compliance with governing regulations and policies, safeguards institutional resources and insure the integrity of all financial systems and data bases.

The Controller's office is responsible for the following functions:

- Accounting and Financial Reporting
- Accounts Payable
- Travel Management
- Cashiering Services
- Accounts Receivable
- Procurement
- Extramural Support Accounting

While responsibility for the major business functions is dispersed throughout UW-Extension, responsibility for the fiscal integrity of the UW-Extension resides with the Chief Business Officer and the Controller.

Internal Audit

UW-Extension's Internal Audit Department is an independent appraisal activity established to conduct reviews of operations and procedures and to report findings and recommendations as a service to UW-Extension management. It examines and evaluates the adequacy and effectiveness of UW-Extension's system of internal control and the quality of performance in carrying out assigned responsibilities. UW-Extension's Internal Auditor reports administratively to the Associate Vice Chancellor for Administrative and Financial Services, but may report audit matters directly to the Chancellor and UW System Administration. Internal Auditor recommends procedures to improve control and operational efficiencies, provides assurance to UW-Extension management that necessary financial and management control are present to safeguard assets, recommends control to prevent and detect fraud and misappropriation of assets and performs liaison functions with various audit agencies.

Annex C includes the Internal Audit Department Charter.

Financial Statements and Other Audited Reports

The University of Wisconsin System publishes an Annual Financial Report containing financial statements prepared in accordance with generally accepted accounting principles as prescribed by the Governmental Accounting Standards Board and the American Institute of Certified Public Accountants' Audit and Accounting guide *Audits of Colleges and Universities*. These financial statements are audited by the State of Wisconsin Legislative Audit Bureau (LAB). Additionally, the University of Wisconsin System, as a member of the Association of Public Land-grant Universities (APLU), complies with their accounting standards and practices.

UW System compiles the Annual Financial Report based on accounting data from the Shared Financial System, and for a variety of reasons it also relies on campuses to submit additional information for selected areas. UW System Administration provides instructions to the campuses for reporting this information.

In addition, LAB performs an organization-wide audit of the UW System in compliance with the federal government's requirements under OMB Circular A-133. This includes an audit of the Schedule of Expenditures of Federal Awards.

Subsequent to the completion of LAB's audit of the Annual Financial Report, UWSA prepares individual financial statements for each campus using the information in the Annual Financial Report. These financial statements are not audited by LAB.

See Annex D for the financial statements for Fiscal Year 2007.

UW System Administration's Office of Operations Review and Audit (OPRA) is responsible for providing objective review and analysis to assure that UW System programs, policies and practices are conducted in accordance with state and federal law and Board of Regents policy. The Office helps ensure University operations are proper, efficient, and effective.

Reporting through the Vice President for Finance, the Director of OPRA is responsible directly to the Board of Regents and provides regular reports that are submitted to the Board of Regents' Business, Finance, and Audit Committee.

By agreement with the Vice President for Finance, the institutional auditors perform certain financial audits formerly performed by OPRA. OPRA coordinates training opportunities for auditors located at the UW institutions and works with the institution auditors to ensure audits are performed in certain core areas.

Code of Conduct

Chapter 19.45 Wisconsin Statutes governs university employees' standard of conduct. It is further codified by Wisconsin Administrative Code, Rules of the Board of Regents – UWS 8; and chapter 24 of Employment Relations Merit Recruitment and Selection manual. Chapter UWEX 8 of the UWEX Faculty and Academic Staff Policies and Procedures Manual sets forth Extension's unclassified staff's code of ethics. A code of ethics for classified staff is included in the UW-Extension Classified Staff Handbook.

Internal Control: Overview

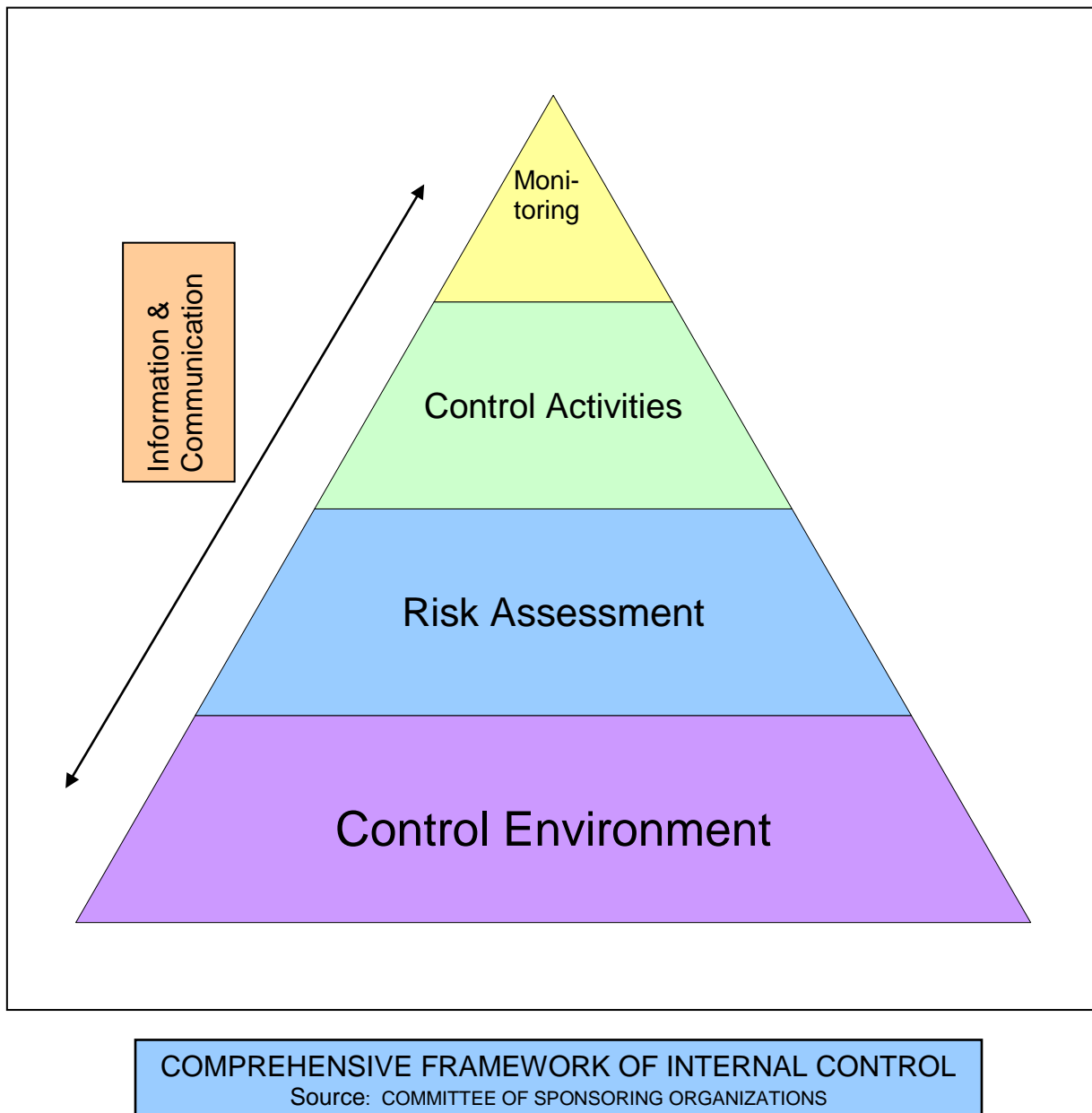
The Committee of Sponsoring Organizations of the Treadway Commission (COSO), is sponsored and funded by 5 main professional accounting associations and institutes; American Institute of Certified Public Accountants (AICPA), American Accounting Association (AAA), Financial Executives International (FEI), The Institute of Internal Auditors (IIA) and The Institute of Management Accountants (IMA).

The COSO framework defines internal control as a process, effected by an entity's board of directors (board of regents), management and other personnel, designed to provide **reasonable assurance** regarding the achievement of **objectives** in the following categories:

- Effectiveness and efficiency of **operations**
- Reliability of **financial reporting**
- **Compliance** with applicable laws and regulations

COSO has established a common definition of internal controls, standards, and criteria against which companies and organizations can assess their control systems.

According to COSO, a comprehensive framework of internal control consists of the following five interrelated components.



- (a) Control Environment. This is the foundation for all other components of internal control encompassing such factors as integrity and ethical values, commitment to competence, board of regent and audit committee participation, management's philosophy and operating style, organizational structure, assignment of authority and responsibility, and human resource policies and practices.

- (b) Risk Assessment. This component identifies, analyzes, and manages the potential risks (i.e. what could go wrong) that could prevent management from achieving its objectives. Change is one factor that can be used to identify risks. Another is inherent risk usually associated with assets that can be readily converted to personal use.
- (c) Control Activities. These are the policies and procedures needed to address the risks identified that could prevent management from achieving its objectives. Control activities generally relate to proper authorization of transactions, security of assets and records, and segregation of incompatible duties. Control activities can be further categorized into programmatic control and administrative and fiscal control.
- (d) Monitoring. It is the responsibility of management to continually monitor control activities to ensure that they function properly and take the necessary corrective action to resolve potential problems or weaknesses in a timely manner. This component also involves evaluating the effectiveness of control, i.e., (1) control is properly designed so they will accomplish their intended purpose and (2) control actually functions as designed.
- (e) Information and Communication. Information provided to staff should be appropriate in content, timely, current, accurate, and accessible. Communication takes such forms as policy manuals, accounting and financial reporting manuals, policy memoranda, and regularly scheduled staff meetings.

Control Environment

The control environment is first of five interrelated components of internal control. It sets the tone of an organization including overall attitude towards adherence to sound business practices, integrity and ethics; influences the attitude and actions of the Board of Regents and management regarding the significance of control; how risk and opportunities are viewed; and affect control consciousness of its people based on how authority is delegated and accountability is enforced. It is the foundation for all other components of internal control by providing discipline and structure.

The Board of Regents has established various policies and procedures for all UW institutions to follow. These policies and procedures as detailed in its web site:

<http://www.uwsa.edu/bor/policies/rpd/>

Risk Assessment

Management's process of identifying potential risks that could result in misstated financial statements and developing actions to address those risks. Areas of

vulnerability if a risk is not addressed, either through a lack of control or insufficient or ineffective control, could be problematic. Exposure may arise from risks in the following areas, which are not inclusive of all possible factors:

Business: Competition, customer/student needs, political factors, legal and regulatory factors, industry factors, and risk of catastrophic loss.

Financial: Compliance, credit, budget and planning, accounting information, financial reporting, taxation, regulatory reporting, and segregation of duties.

Operational: Student/customer satisfaction, knowledge capital, efficiency, performance gaps, partnering, compliance, outsourcing, communications, management fraud, employee/third party fraud, illegal acts, and inaccurate measurements.

Information Technology: Technology innovation, change readiness, relevance, integrity, access, and infrastructure.

Public and Political Sensitivity: Considers the impact if a business process or program is exposed to adverse publicity, both publicly and politically. Also includes compliance, which is discussed further below.

Compliance Requirements: Considers the extent and the impact of laws and regulations on the business program or process being considered. For example, is a business program or process subject to complex, extensive or limited regulation (federal, state, UW System, UW-Extension internal policies, or independent organizations such as the NCAA), and who are the regulatory bodies who have the most influence on the process?

Information and Reporting: The extent to which various types of information on a business program and/or process is available and disseminated to management or public. For example, is information decentralized and difficult to gather into a meaningful format, or is it highly centralized and elaborated, with detailed reports that are available?

Organization Change and Growth: The extent to which a business process or program is affected by changes in the organization, or itself causes changes to the organization. For example, a process or program may change frequently and have a significant impact on the University, while on the other hand, a process or program may be fairly static and is not significantly affected by change, or cause change in other areas.

Consideration of Internal Control Over Key Subcycles: The UW institutions have identified the following major transaction cycles pertinent to their operations:

- Revenue Cycle
- Disbursements Cycle
- Cost Allocations Cycle
- Property Control Cycle
- Cash and Investments Mgmt Cycle
- Budget Management Cycle
- Debt Management Cycle
- Financial Reporting Cycle

Risk assessment on revenue and expenditures subcycles should consider five factors:

1. The materiality of the dollars associated with that type of transaction;
2. Known problems such as inadequate separation of duties, prior audit findings, etc.;
3. Management/process factors such as complexity of the operation, recent changes in process, personnel turnover, management quality, prior history, quality of internal control (to the extent known), source of input, degree of automation, impact of inadequate control, etc.;
4. Time elapsed since last audit coverage of the subcycle;
5. Public factors such as political sensitivity the potential impact of adverse publicity; regulatory or compliance concerns.

Internal Audit also performed a high-level review of the adequacy of internal control over the following subcycles, in order to identify the existence of any areas of significant residual risk (risk that is unaddressed by internal control).

- Purchasing Cards
- Capital Equipment
- Nonpayroll Expenses
- General Ledger Journal Entries
- Human Resources

The objectives and procedures of these reviews are included in Annex E.

Control Activities

These are the activities usually thought of as "the internal controls." They include such things as segregation of duties, account reconciliations and information processing controls that are designed to safeguard assets and enable an organization to timely prepare reliable financial statements. Control activities include a variety of policies, procedures, practices or processes that are designed to ensure that necessary actions are taken to enforce the policies established by regulators or management. Examples of these types of activities are as follows:

- Review of operating reports – This activity includes the monthly reconciliation of accounts to ensure accounts are balanced with the detailed ledgers so that transactions that were not authorized could be identified and correction or investigation of errors could occur.
- Reviews of accounts - This activity requires that the SFS system be reviewed to compare actual expenses vs. budget and to look for unusually high expenses in object codes to determine if all transactions incurred were as intended.

- Reviews of accounting records – This activity includes checking accounting records to make sure they are neat, in proper order and are kept current and that all entries to the accounting system are accurate, complete and were properly authorized. This will speed up the payment, reimbursement or recording of the activity and result in an efficient processing of the document
- Reviews of control of liquid type assets like cash, inventory or equipment – Physical controls are essential for adequate control of liquid type assets. This can take the form of secured (locked) locations for the storage of inventory or equipment, safes or vaults for the storage of cash and periodic physical counts of cash, inventory and equipment and the comparison of the value of those counts to the records.
- Review of cash handling - Segregation of duties is one of the more important of this type of activity. It provides for the division or segregation of duties among different people to reduce the risk of undetected errors or inappropriate actions. Care must be taken to avoid improperly delegating responsibilities to one individual because this can create a situation whereby that one individual controls all aspects of a transaction – the purchase, payment and receipt of goods without any oversight.

Most of the relevant control associated with processing the financial transactions of UW-Extension takes place at UW-Extension. The major policies, procedures, practices and processes involved in control activities that can be used to help enforce and achieve departmental objectives are detailed on various web pages. See “Information and Communication” section below for web links.

To assess and document the internal control objectives, the UW institutions have agreed upon a format detailed in Annex E. This format, control matrices, for documenting internal control activities will be adopted as an adjunct to documentation that may exist in procedure manuals, audit programs, and audit workpapers. Control matrices are an efficient way of understanding key controls that address specific risks. So the control matrices include:

- List all the assertions and risks for a subcycle or an account or line item
- List all the key controls which address the assertion
- Relate the risks with the controls which address the risks
- Type of Control (manual or automated)
- Objective and significance of control.

Monitoring

Monitoring is the process that assesses the quality of internal control performance over time and taking actions as necessary to ensure it continues to address the risks of the organization. Monitoring is effective when it leads to the identification and correction of control weaknesses *before* they **materially** affect the achievement of the organization’s objectives. Monitoring is a cost-effective approach to providing timely information about

the continued effectiveness of an internal control system. As such, effective monitoring is a net benefit to organizations and their stakeholders.

Effective and efficient monitoring is best achieved by:

1. Establishing a foundation for monitoring, including a proper tone at the top, organizational structure and a baseline understanding of internal control effectiveness
2. Designing and executing monitoring procedures that seek to evaluate "persuasive" information about "key controls" addressing "meaningful risks" to organizational objectives
3. Assessing results and reporting them to appropriate parties

Once every three years, in accordance with the Cooperative Agreement on Accounting, Auditing and Internal Accounting Control Activities between UW System Administration and the UW-Extension, the Chief Business Officer for the University of Extension will certify to the UW System Vice President for Finance that Extension's internal accounting control have been reviewed and that any material weaknesses in these control have been corrected. Plans to correct weaknesses will also be communicated to the UW System Vice President for Finance. The Business Services department is responsible for ongoing monitoring built-in through independent reconciliations and review of exception reports.

Internal Control will also be monitored during the course of UW-Extension internal audits which test for compliance with Federal, State, and UW System requirements. UW-Extension auditor performs periodic review of transactions of basic sampling techniques to provide a reasonable level of confidence that control are functioning. The Internal Auditor meets with division management to evaluate the condition of the program and control. A copy of the audit report is sent to the Controller.

The Associate Vice Chancellor of Administrative and Financial reviews the results of audit reports and periodically assesses the adequacy of corrective action on high-risk areas. The Controller also receives a copy of the audit report to keep apprised of the state of the internal control. Internal control systems are routinely subject to assessment by external audit entities and also in connection with audits performed by OPRA.

Information and Communication

Information and communication are the identification, capture, exchange of information in a form and time frame that enable people to carry out their responsibilities, and are essential to effecting control. The internal and external reporting process and includes an assessment of the technology environment. Each UW institution will include the following information and communication activities in their internal control plan:

- Accounting system provides for separate identification of Federal and non-Federal transactions and allocation of transactions applicable to both.
- Adequate source documentation exists to support amounts and items reported.
- Recordkeeping system is established to ensure that accounting records and documentation retained for the time period required by applicable requirements; such as provisions of laws, regulations, contracts or grant agreements applicable to specific programs.
- Reports provided timely to managers for review and appropriate action.
- Accurate information is accessible to those who need it.
- Reconciliations and reviews ensure accuracy of reports.
- Established internal and external communication channels.
- Employees' duties and control responsibilities effectively communicated.
- Channels of communication for people to report suspected improprieties established.
- Actions taken as a result of communications received.

Information related to internal control is communicated primarily via the Internet.

UW-System Administration (UWSA)

UWSA has produced various documents including the Preaudit Manual; Financial and Administrative Policies; Financial Reports; Financial Reporting Due Dates; information on the UW System Shared Financial System; as well as links to other external financial sites and has made this information available on the UW-System web site at:

<http://www.uwsa.edu/fadmin/>.

Financial administration policies which specifically address internal control issues include:

- Purchasing Responsibility and Authority (G8)
- Uninsured Personal Property Losses or Damages (F41)
- Breach of Fiscal Integrity (F16)
- Loss Fund Operations (F35)

Business Services

The Office of Business Services of the UW-Extension has posted on its web site a variety of documents that relate to internal control at its website at:

<http://www.uwex.edu/business-services/>

Financial administrative policies or manuals addressing internal control issues include:

- Business Services Policy and Procedure Manual
- Account Code Manual
- The Extramural Support Procedures Manual
- Procurement Policies and Procedures
- Processing of Financial Transactions Procedures
- Accounts Payable Procedures
- Cashier Services Policy and Procedures Manual
- Purchasing Card Manual

Internal Audit

The Internal Audit Department also posted on its web site a variety of internal audit issues at:

<http://uwex.uwc.edu/admin-services/audit/>

Internal control related issues include:

- UW-Extension Internal Control Plan
- Charter
- Various presentations including Ethics
- Self assessment tools

Statement of Support for Internal Accounting Control

**Chancellor of the University of Wisconsin-Extension
Associate Vice Chancellor – Administrative & Financial Services
Controller – Business Services**

Recognizing that a vital component of UW-Extension’s mission is to safeguard its assets and ensure the proper use of resources, the chief administrative officers of UW-Extension accept responsibility for the implementation and utilization of this Internal Control Plan.

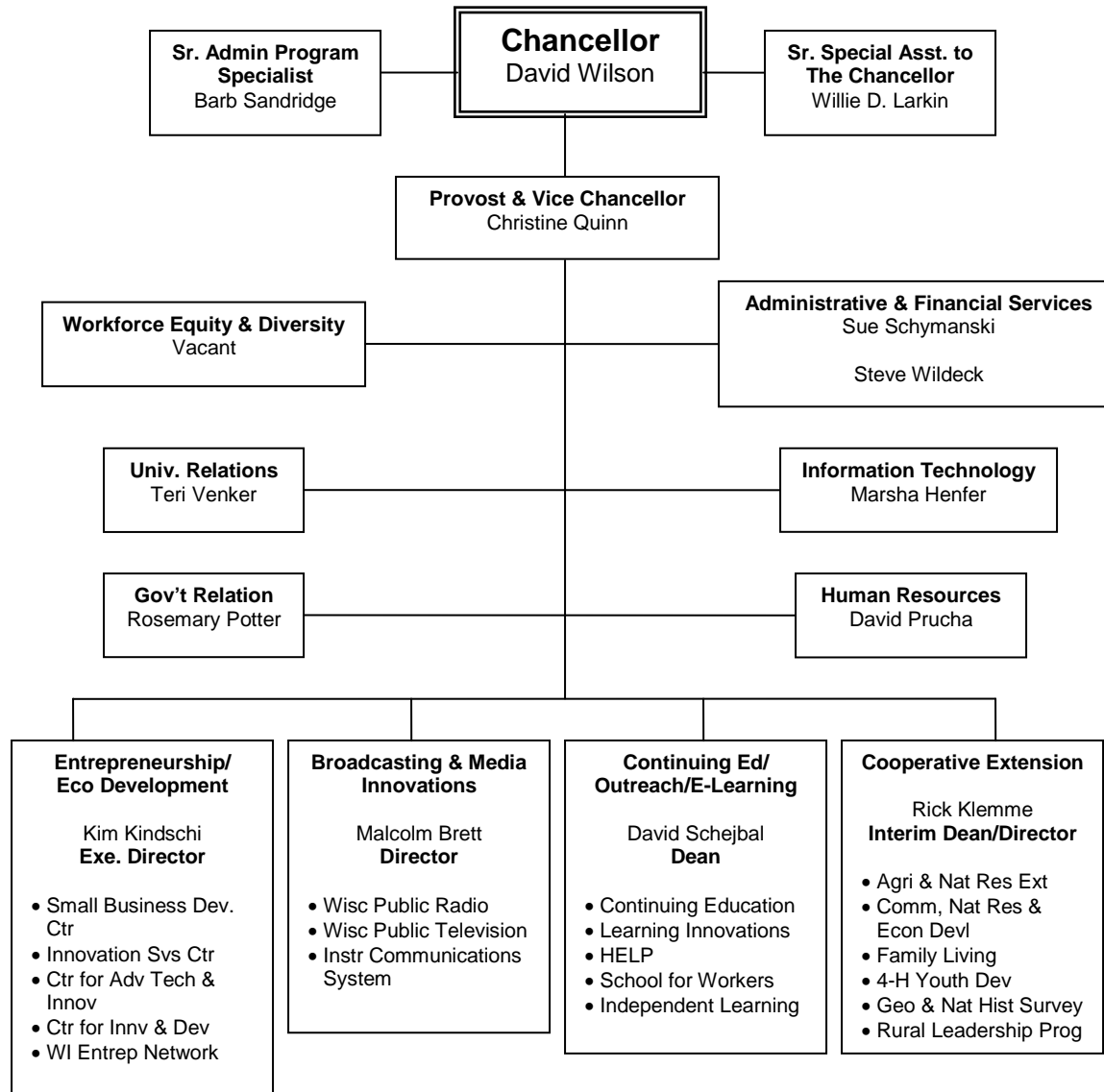
I affirm the UW-Extension’s total and ongoing commitment to implementing and maintaining appropriate safeguards over the financial assets placed in our care.

| | |
|---|------|
| | |
| David Wilson UW-Extension Chancellor | Date |

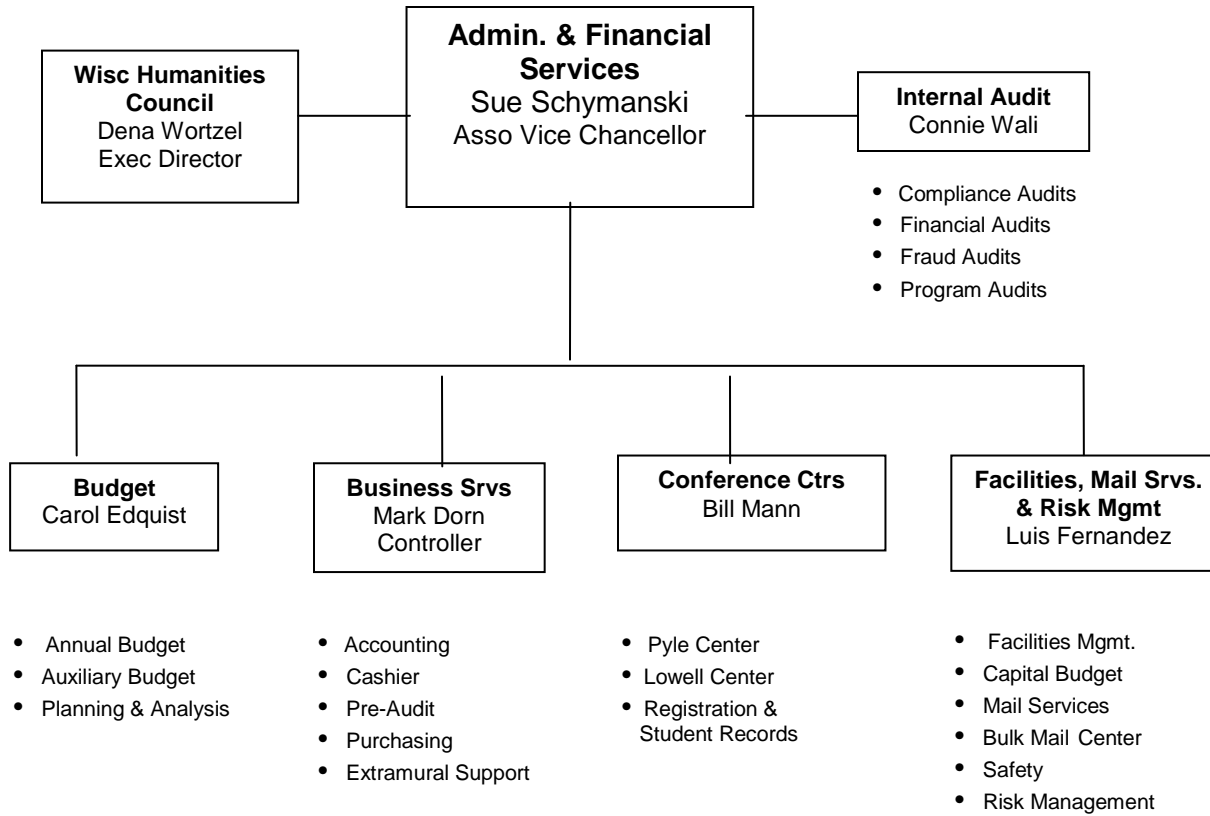
| | |
|---|------|
| | |
| Sue Schymanski Asso. Vice Chancellor – Administrative & Financial Svcs | Date |

| | |
|---|------|
| | |
| Mark Dorn Controller – Business & Financial Services | Date |

Annex A - UW-Extension Executive Level Organization Chart



Annex B - UW-Extension Admin & Fin Svcs Organization Chart



Annex C – UW-Extension Charter

Introduction

This charter defines the policy of the University of Wisconsin-Extension (UW-Extension) regarding the Internal Audit Department and authorizes its access to records, personnel, and physical properties relevant to the performance of audits, and to define the scope of internal auditing activities.

Purpose of Internal Audit Department

Internal auditing is an independent appraisal activity established to evaluate the effectiveness of processes, internal control, and systems, and identify opportunities for improvement. A major purpose of the internal audit function is the prevention and detection of fraud, embezzlement, and misappropriation of assets.

Objective of Internal Audit Department

It is the policy of the UW-Extension to provide an internal auditing function to assist management by reviewing all operations at appropriate intervals, and provide analyses, appraisals, recommendations, counsel and information concerning the activities reviewed.

Authority of Internal Audit Department

Internal Audit reports administratively to the Associate Vice Chancellor of Administrative & Financial Services; however, may report audit matters directly to the Chancellor or to University of Wisconsin System Administration.

In the performance of audits, the Internal Audit is granted the authority to audit all parts of the institution and shall have full and complete access to any of the institution's records, physical properties and personnel. Documents and information given to the auditors during a periodic review will be handled in the same prudent and confidential manner as by those employees normally accountable for them and exercise discretion and assure the safekeeping and confidentiality of audit matters.

Internal Audit Department will have no direct responsibility for or the authority over, any of the activities reviewed. Therefore, an internal audit review in no way relieves management of any assigned responsibilities. Internal Audit Department should make recommendations for new or additional control or procedures, but not develop or install them, prepare records or engage in any activities which they would normally be required to review.

The Internal Audit Department should not perform non-audit work except under unusual circumstances because performance of line responsibilities may compromise objectivity.

All Internal Auditing endeavors are to be conducted in accordance with University policies as well as the Code of Ethics and the Standards for the Professional Practice of Internal Auditing promulgated by The Institute of Internal Auditors.

Responsibilities of Internal Audit Department

The Internal Audit Department has responsibility for:

- Developing and maintaining a comprehensive internal auditing program for evaluating the financial and operational systems and procedures for all UW-Extension activities.
- Development of an annual audit plan in consultation with the Associate Vice Chancellor of Administrative & Financial Services.
- Examining financial transactions for accuracy and evaluating compliance with internal policies and procedures, UW System policies, and governmental laws and regulations.
- Ascertaining the adequacy of control for safeguarding assets and, when appropriate, verifying the existence of assets.
- Appraising the timeliness, reliability, and usefulness of institutional records and reports.
- Evaluating the cost effectiveness and efficiency of institutional operations and the adequacy of meeting intended program objectives.
- Preparation of reports for each audit whose findings and recommendations have been discussed with the management of the audited operation, responded to by that management, presented to the Associate Vice Chancellor of Administrative & Financial Services with a copy forward to the UW System Office of Operations Review & Audit.
- Serving as a liaison with external auditors and coordinating audit efforts with UW System Internal Audit to preclude duplication of effort and increase coverage of auditable areas.
- Conducting follow-up reviews on audit reports issued by UW System, Legislative Audit Bureau, or other external agencies.
- Serving on committees as appointed or elected.
- Maintaining technical competence through continuing education and active involvement in professional activities.
- Ensure any fiscal misconduct or conflicts of interest are reported in accordance with System Administration policy.
- Involvement in the review of any new system, developed internally or purchased, to determine the adequacy of internal control prior to the implementation of that system.

Annex D - Financial Statements for FY 2007

Statements of Net Assets

| University of Wisconsin System - EXTENSION | June 30, 2007 | June 30, 2006 |
|--|------------------|------------------|
| ASSETS | | |
| Current Assets: | | |
| Cash and Cash Equivalents | \$ 21,960,838.74 | \$ 17,096,186.56 |
| Accounts Receivable, Net | \$ 10,694,454.58 | \$ 11,798,671.86 |
| Student Loans Receivable, Net | \$ - | \$ - |
| Capital Lease Receivable | \$ - | \$ - |
| Inventories | \$ 226,663.00 | \$ 322,061.26 |
| Prepaid Expenses | \$ 1,119,887.79 | \$ 984,633.98 |
| Deferred Charges | \$ 10,812.07 | \$ 7,653.72 |
| Total Current Assets | \$ 34,012,656.18 | \$ 30,209,207.38 |
| Noncurrent Assets | | |
| Endowment Investments | \$ 6,885,333.37 | \$ 5,473,431.25 |
| Student Loans Receivable, Net | \$ - | \$ - |
| Capital Lease Receivable | \$ - | \$ - |
| Land | \$ 418,982.86 | \$ 418,982.86 |
| Improvements Other Than Buildings, Net | \$ 1,153,205.65 | \$ 1,325,125.19 |
| Construction in Progress | \$ 60,911.57 | \$ 1,306,342.23 |
| Buildings, Net | \$ 20,012,468.07 | \$ 17,930,468.04 |
| Equipment, Net | \$ 4,070,678.80 | \$ 3,931,804.10 |
| Library Holdings | \$ - | \$ - |
| Total Noncurrent Assets | \$ 32,601,580.32 | \$ 30,386,153.67 |
| TOTAL ASSETS | \$ 66,614,236.50 | \$ 60,595,361.05 |
| LIABILITIES | | |
| Current Liabilities | | |
| Accounts Payable and Accrued Liabilities | \$ 4,079,599.77 | \$ 3,302,134.27 |
| Notes and Bonds Payable | \$ 108,467.86 | \$ 68,425.17 |
| Capital Lease Obligations | \$ 14,301.00 | \$ 19,612.13 |
| Deferred Revenue | \$ 3,418,714.42 | \$ 3,153,765.56 |
| Compensated Absences | \$ 2,791,228.88 | \$ 2,651,661.57 |
| Deposits of Student Organizations | \$ - | \$ - |
| Total Current Liabilities | \$ 10,412,311.93 | \$ 9,195,598.70 |
| Noncurrent Liabilities | | |
| Notes and Bonds Payable | 1,986,042.59 | 929,326.91 |
| Capital Lease Obligations | - | 18,804.66 |
| Compensated Absences | 2,565,192.73 | 2,155,207.12 |
| Total Noncurrent Liabilities | 4,551,235.32 | 3,103,338.69 |
| TOTAL LIABILITIES | 14,963,547.25 | 12,298,937.39 |
| NET ASSETS | | |
| Invested in Capital Assets, net of Related Debt | 23,607,435.50 | 21,459,542.91 |
| Restricted for | | |
| Nonexpendable | 5,170.43 | 4,298.85 |
| Expendable | 12,923,825.31 | 10,167,910.42 |
| Student Loans | - | - |
| Other | 6,073,146.03 | 7,237,925.33 |
| Unrestricted | 9,041,111.98 | 9,426,746.15 |
| TOTAL NET ASSETS | 51,650,689.25 | 48,296,423.66 |

The accompanying notes to the financial statements are an integral part of these statements.

The University of Wisconsin – Extension
Internal Control Plan – March 2009

Statements of Revenues, Expenses and Changes in Net Assets

University of Wisconsin System - EXTENSION

Year ended June 30, 2007

Year ended June 30, 2006

OPERATING REVENUES

| | | | | |
|--|----|----------------------|----|----------------------|
| Student Tuition and Fees (net of Scholarship Allowances of \$0 and \$0, respectively) | \$ | 42,379.57 | \$ | 52,417.99 |
| Federal Grants and Contracts | \$ | 12,170,075.15 | \$ | 15,514,805.77 |
| State, Local and Private Grants and Contracts | \$ | 32,110,744.90 | \$ | 27,174,483.70 |
| Sales and Services of Educational Activities | \$ | 11,266,188.03 | \$ | 8,611,365.85 |
| Sales and Services of Auxiliary Enterprises (net of Scholarship Allowances of \$0 and \$0, respectively) | \$ | 0.13 | \$ | - |
| Sales and Services to UW Hospital Authority | \$ | - | \$ | - |
| Student Loan Interest Income and Fees | \$ | - | \$ | - |
| Other Operating Revenue | \$ | 47,485.92 | \$ | 36,880.63 |
| Total Operating Revenues | \$ | 55,636,873.70 | \$ | 51,389,953.94 |

OPERATING EXPENSES

| | | | | |
|---------------------------------|----|----------------------|----|----------------------|
| Salary and Fringe Benefits | \$ | 76,588,642.20 | \$ | 74,119,690.36 |
| Scholarship and Fellowships | \$ | - | \$ | - |
| Supplies and Services | \$ | 19,016,674.16 | \$ | 17,106,872.72 |
| Other Operating Expenses | \$ | 597,215.97 | \$ | 745,675.81 |
| Depreciation | \$ | 1,930,182.61 | \$ | 1,739,433.33 |
| Total Operating Expenses | \$ | 98,132,714.94 | \$ | 93,711,672.22 |

OPERATING INCOME (LOSS) \$ (42,495,841.24) \$ (42,321,718.28)

NON-OPERATING REVENUES AND EXPENSES

| | | | | |
|--|----|-----------------|----|----------------|
| State Appropriations | \$ | 52,238,984.48 | \$ | 52,365,732.01 |
| Gifts | \$ | 2,483,791.99 | \$ | 2,695,813.26 |
| Investment Income (net of Investment Expense) | \$ | 1,611,590.13 | \$ | (139,613.43) |
| Loss on Disposal of Capital Assets | \$ | - | \$ | (9,520.00) |
| Interest on Indebtedness | \$ | (76,084.55) | \$ | (56,237.66) |
| Transfer to DOA | \$ | (1,245,913.96) | \$ | (1,099,678.76) |
| Other | \$ | (10,660,394.80) | \$ | (9,147,062.35) |
| Income Before Capital and Endowment Additions/Deductions | \$ | 1,856,132.05 | \$ | 2,287,714.79 |
| Capital Contributions | \$ | 1,540,436.75 | \$ | 1,448,370.32 |
| Additions to Permanent Endowment | \$ | - | \$ | 20.00 |

INCREASE IN NET ASSETS \$ 3,396,568.80 \$ 3,736,105.11

NET ASSETS

| | | | | |
|-----------------------------------|----|----------------------|----|----------------------|
| Net Assets - beginning of period | \$ | 48,296,423.66 | \$ | 44,560,318.55 |
| Prior Period Adjustment | \$ | (42,303.21) | \$ | - |
| NET ASSETS - end of period | \$ | 51,650,689.25 | \$ | 48,296,423.66 |

The accompanying notes to the financial statements are an integral part of these statements.

The University of Wisconsin – Extension
Internal Control Plan – March 2009

Statements of Cash Flows

University of Wisconsin System - EXTENSION

Year ended June 30, 2007

Year ended June 30, 2006

Cash Flows from Operating Activities

| | | | | |
|--|----|------------------------|----|------------------------|
| Student Tuition and Fees | \$ | 277,950.58 | \$ | 108,781.40 |
| Federal, State, Local and Private Grants & Contracts | \$ | 47,009,303.27 | \$ | 39,163,687.30 |
| Sales and Services of Educational Activities | \$ | 11,004,667.22 | \$ | 8,774,101.20 |
| Sales and Services of Auxiliary Enterprises | \$ | (1,426,346.73) | \$ | 383,449.61 |
| Sales and Services to UW Hospital Authority | \$ | - | \$ | - |
| Payments for Salaries and Fringe Benefits | \$ | (75,588,164.14) | \$ | (78,034,927.32) |
| Payments to Vendors and Suppliers | \$ | (18,596,814.68) | \$ | (14,830,884.58) |
| Payments for Scholarships and Fellowships | \$ | - | \$ | - |
| Student Loans Collected | \$ | - | \$ | - |
| Student Loan Interest and Fees Collected | \$ | - | \$ | - |
| Student Loans Issued | \$ | - | \$ | - |
| Other Revenue (Expense) | \$ | (556,847.55) | \$ | 197,532.22 |
| Net Cash Used in Operating Activities | \$ | (37,876,252.03) | \$ | (44,238,260.17) |

Cash Flows from Investing Activities

| | | | | |
|---|----|-------------------|----|-------------------|
| Interest and Dividends on Investments, Net | \$ | 627,252.07 | \$ | (967,565.71) |
| Proceeds from Sales and Maturities of Investments | \$ | 4,213,910.01 | \$ | 10,885,924.54 |
| Purchase of Investments | \$ | (4,640,187.37) | \$ | (9,722,494.34) |
| Net Cash Provided by Investing Activities | \$ | 200,974.71 | \$ | 195,864.49 |

Cash Flows from Capital and Related Financing Activities

| | | | | |
|--|----|---------------------|----|-----------------------|
| Proceeds from Issuance of Capital Debt | \$ | 2,526,810.26 | \$ | 1,262,225.32 |
| Gifts and Other Receipts | \$ | 177,422.50 | \$ | 186,645.00 |
| Purchase of Capital Assets | \$ | (2,767,862.38) | \$ | (2,591,849.08) |
| Principal Payments on Capital Debt and Leases | \$ | (89,918.12) | \$ | (105,014.75) |
| Interest Payments on Capital Debt and Leases | \$ | (80,687.26) | \$ | (64,179.72) |
| Net Cash Used in Capital and Related Financing Activities | \$ | (234,235.00) | \$ | (1,312,173.23) |

Cash Flows from Noncapital Financing Activities

| | | | | |
|---|----|----------------------|----|----------------------|
| State Appropriations | \$ | 52,238,984.48 | \$ | 52,365,732.01 |
| Gifts and Other Receipts | \$ | (8,176,602.81) | \$ | (6,451,749.09) |
| Transfer to DOA | \$ | (1,245,913.96) | \$ | (1,099,678.76) |
| Additions to Permanent Endowments | \$ | - | \$ | 20.00 |
| Student Direct Lending Receipts | \$ | - | \$ | - |
| Student Direct Lending Disbursements | \$ | - | \$ | - |
| Net Cash Provided by Noncapital Financing Activities | \$ | 42,816,467.71 | \$ | 44,814,324.16 |

Net Increase in Cash and Cash Equivalents

| | | | | |
|--|----|----------------------|----|----------------------|
| Net Increase in Cash and Cash Equivalents | \$ | 4,906,955.39 | \$ | (540,244.75) |
| Cash and Cash Equivalents - beginning of year | \$ | 17,096,186.56 | \$ | 17,636,431.31 |
| Prior Period Adjustment | \$ | (42,303.21) | \$ | - |
| Cash and Cash Equivalents - end of year | \$ | 21,960,838.74 | \$ | 17,096,186.56 |

Reconciliation of Operating Income (Loss) to Net Cash Used in Operating Activities

| | | | | |
|---|----|------------------------|----|------------------------|
| Operating Income (Loss) | \$ | (42,495,841.24) | \$ | (42,321,718.28) |
| <i>Adjustments to Reconcile Operating Income (Loss) to Net Cash Used in Operating Activities:</i> | | | | |
| Depreciation Expense | \$ | 1,930,182.61 | \$ | 1,739,433.33 |
| Changes in Assets and Liabilities: | | | | |
| Receivables, net | \$ | 1,004,120.20 | \$ | (2,257,627.44) |
| Inventories | \$ | 95,398.26 | \$ | 12,029.74 |
| Prepaid Expense | \$ | (135,253.81) | \$ | (42,790.93) |
| Deferred Charges | \$ | - | \$ | - |
| Accounts Payable and Accrued Liabilities | \$ | 910,640.17 | \$ | (1,694,937.76) |
| Deferred Revenue | \$ | 264,948.86 | \$ | 240,901.04 |
| Compensated Absences | \$ | 549,552.92 | \$ | 86,450.13 |
| Net Cash Used in Operating Activities | \$ | (37,876,252.03) | \$ | (44,238,260.17) |

Noncash Investing, Capital and Financing Activities

| | | | | |
|---|----|------------|----|--------------|
| Capital Leases (Initial Year): | | | | |
| Fair Market Value | \$ | - | \$ | - |
| Current Year Cash Payments | \$ | - | \$ | - |
| Gifts-In-Kind | \$ | - | \$ | - |
| Net Change in Unrealized Gains and Losses | \$ | 659,283.64 | \$ | (214,456.10) |

Annex E - Internal Control Matrices

E-1 Control Matrix – Revenues

| NO. | INTERNAL CONTROL | RISKS | KEY CONTROL POINTS | | |
|-----|--|---|---|--|--|
| | | | Operating Controls | Monitoring Controls | Oversight Controls |
| | Listed below are the sub-processes within the overall revenues process and what we are trying to control for within this sub-function. | This column lists risks inherent to the process which might cause inaccurate data or inaccurate activity. | | | |
| 1 | Fees are properly calculated and billed | <p>Failure to comply with BOR, UW System, or institutional policies</p> <p>Favoritism to certain participants</p> <p>Over/under collection of revenue</p> | <p>The assessment of charges are managed or approved by the division.</p> <p>Division Accounting is responsible for updating the rate tables.</p> <p>Fee assessment procedures are documented.</p> <p>The responsibility of billing is segregated from collections and accounting system postings (Business Services).</p> | <p>Departments issue invoices.</p> <p>Business Services handles account receivables and process remittances</p> | <p>Fees are determined by individual departments and are subject to budgetary approval at the division.</p> |
| 2 | Receipts are properly credited and debited in a secure manner to the appropriate business unit, fund, account, and class within SFS and to the appropriate accounts receivable balance where applicable. | <p>Receipts are lost or stolen</p> <p>Inaccurate financial reporting</p> | <p>Reconciliations are performed between SFS and the Business Services Accounting records.</p> <p>Reconciliations are performed between the systems and the deposits.</p> <p>Reconciliation variances are documented and resolved in a timely manner.</p> <p>Offices are physically secure, including access controls and lock boxes.</p> <p>System edit checks preclude inconsistent or incompatible codes.</p> <p>Receipts collected by the Cashier's office are deposited within 7 days.</p> | <p>Reconciliations are reviewed and approved by a supervisor.</p> <p>The Controller's office facilitates segregation of duties by controlling access to People Soft.</p> | <p>Management/analytical reviews are conducted.</p> <p>Daily deposits are not entered directly into SFS; they are entered into the Cashier's office system which is uploaded into SFS.</p> |

The University of Wisconsin – Extension
Internal Control Plan – March 2009

| | | | | | |
|---|---|--|--|--|--|
| 3 | Refunds to participants are properly credited and debited to the appropriate accounts | <p>Failure to comply with BOR, UW System, or institutional policies</p> <p>Failure to comply with federal regulations, possibly resulting in audit findings, questioned costs, and loss of federal funding</p> | <p>Process to authorize individuals to process refunds is documented.</p> <p>Only authorized individuals are permitted to process refunds.</p> <p>Refund calculations are adequately documented and supported.</p> <p>Refund procedures are adequately documented.</p> <p>Refunds are provided to participants. If an award is being adjusted, amounts are returned to the entity providing the award.</p> | <p>Refunds are subject to review and supervisory approval.</p> <p>Any changes to enrollment that might be subject to timing issues are reviewed to determine if the student is eligible to receive a refund.</p> | Refund policies are documented on program announcements, brochures, and catalogs. |
| 4 | Journal entries to adjust or correct revenue are in accordance with UW criteria | <p>Inaccurate financial reporting</p> <p>Audit adjustments/qualifications</p> <p>Inaccurate budget and marginal tuition revenue analyses</p> | <p>Only authorized individuals are permitted to process journal entries.</p> <p>Journal entries are adequately documented and supported.</p> <p>Journal entries may be made in the cashier system, which interfaces to SFS.</p> <p>Accounting Services completes any remaining entries.</p> | Journal entries are subject to review and supervisory approval | |
| 5 | Revenue and related receivables are correctly reported within the institution and to UWSA on a periodic basis | <p>Inaccurate financial reporting</p> <p>Audit adjustments/qualifications</p> <p>Inaccurate budget and marginal tuition revenue analyses</p> | <p>Staff is experienced and knowledgeable of the system and institutional operations.</p> <p>Revenue is reported daily in SFS.</p> | Separation of duties is maintained so that different personnel enter payments and reconcile those entries. | Management/analytical reviews are conducted for consistency, comparability, and reasonableness by institutional and UWSA staff |
| 6 | Account receivables are promptly collected | <p>Accounts may become uncollectable if not properly pursued</p> <p>Misappropriation of funds</p> | There is a standard monthly billing cycle to collect all accounts receivable. | Adjustments to participants accounts, including write-offs, require supervisory or UWSA approval | |

E-2 Control Matrix – Disbursements Nonpayroll

| NO. | INTERNAL CONTROL | RISKS | KEY CONTROL POINTS | | |
|-----|--|---|---|---|--------------------|
| | | | Operating Controls | Monitoring Controls | Oversight Controls |
| | Listed below are the sub-processes within the overall Disbursement process and what we are trying to control for within this sub-function. | This column lists risks inherent to the process which might cause inaccurate data or inaccurate activity. | | | |
| 1 | Duplicate payments are not made | <ol style="list-style-type: none"> 1. UW may lose the overpayment funds if not returned by the vendor. 2. Failure to comply with UW System, Board of Regents and institution policies. 3. Duplicate payment is made from department with insufficient funds. 4. Payments are processed for an invalid or fraudulent vendor. | <p>The pre-audit process requires an original invoice to pay, and it is unlikely that the vendor will issue multiple original invoices for the same charges. Accounts payable staff verify original vendor invoice, verify authorized signature is appropriate for funding coding being charged, and that the vendor has been set up in the system</p> <p>If copied, faxed, e-mailed invoice is received, staff review recent payments for vendor to determine if this invoice has been paid.</p> <p>The AP staff are trained to pay from original invoices only, not statements received from the vendor. Statements are followed up on to determine if unpaid invoices have been received or paid.</p> <p>AP staff enter the invoice number in the invoice field to allow the system to flag duplicates.</p> <p>PeopleSoft prompts the AP staff when a duplicate invoice number is entered for that vendor.</p> | Because staff pay from originals, or in rare cases duplicate with other procedures completed, it is unlikely that duplicate payments will occur | |
| 2 | Payments made to outside vendors are paid in compliance with all State, UW System, UW-Extension and outside funding agency policies. | <ol style="list-style-type: none"> 1. UW's reputation could be damaged. 2. Possible audit finding or citation. 3. Loss of federal grant funding or the requirement to pay back federal grant funds with other department funds. | <p>AP staff training on UW System policies for allowable expenses.</p> <p>Staff are trained on documentation that must accompany certain types of expenses.</p> <p>Policy papers are available on our web site, or through links to review for appropriate payments.</p> | Staff are trained in allowable expenses, are aware of the policies governing expenses, and have access to search policies when needed. | |

The University of Wisconsin – Extension
Internal Control Plan – March 2009

| | | | | | |
|---|---|---|--|---|--|
| | | | <p>Staff seek assistance from supervisors if unsure about policy interpretation.</p> <p>Extramural support funds (133, 144, 161, 233) are reviewed by OES staff for appropriateness before payment.</p> | | |
| 3 | Account coding is correct and consistent. | <ol style="list-style-type: none"> 1. Failure to comply with UW System, Board of Regents and institution policies. 2. UW's reputation could be damaged. 3. Wrong department or expense account charged. 4. Year end reporting is inaccurate | <p>Buyers or Purchasing Department code all transactions. BS reviews coding.</p> <p>Chargebacks coming from service departments use standard account coding for that area, and are provided charge codes by departments when services are ordered.</p> <p>Departments have access to WISDM to review expenses charged against their department codes, and forward questions or corrections to Financial Services.</p> | Trained staff limit the possibility for incorrect codes to be used. | |
| 4 | Invoices and payment documents are authorized and approved by a qualified signer for the department | <ol style="list-style-type: none"> 1. Payments are processed for an invalid vendor. 2. Payments are authorized by staff without authority to do so. 3. Payments are paid from a department with sufficient funds, resulting in a negative cash balance. 4. Goods and/or services are not received by the department submitting the information. 5. Fraudulent charges/invoices could be submitted. | <p>Authorized signor list is maintained by Financial Services for each department code.</p> <p>Staff processing payments review authorized signor signatures for actual signature (not stamp) and if it matches the authorized signor list for that department code.</p> <p>Departments have access to WISDM to review expenses charged against their department codes, and forward questions or corrections to Financial Services.</p> <p>Payment with inappropriate signatures are returned to the authorized signor for review and signature.</p> | Signatures are reviewed and the payment is only processed if appropriate. | |

The University of Wisconsin – Extension
Internal Control Plan – March 2009

| | | | | | |
|---|--|--|---|---|--|
| 5 | Invoices are paid in a timely manner. | <ol style="list-style-type: none"> 1. Not taking advantage of a discount offered by vendors for timely payment. 2. UW's reputation could be damaged. 3. Failure to comply with State, UW System, Board of Regents and UW-Extension policies. 4. Payment of Finance/interest charges for late payments. | <p>Invoices are paid as soon as the pre-audit procedures are completed and staff are mindful of meeting the 30 day statutory requirement for payment.</p> <p>The default when entering a voucher on PeopleSoft is DUR (due on receipt). When these payment terms are selected, the check will print the next day.</p> <p>Checks are printed and mailed several times a week.</p> <p>Checks are mailed directly to the vendor.</p> | <ol style="list-style-type: none"> a. Timely processing and mailing of payments once documentation is received ensure timely payment. b. If departments do not forward the invoices timely, payments will not be made on time. c. Delays caused by a dispute over the invoice require a Dispute Letter to be immediately sent to the vendor. | |
| 6 | Vendors paid through the AP process are valid companies or individuals | <ol style="list-style-type: none"> 1. Fraudulent vendor is set up in the payment system. 2. Incorrect 1099 could be issued. 3. Fraudulent payments could be made for services never provided. 4. UW's reputation could be damaged. | <p>Vendor file is maintained by BS.</p> <p>W-9 is required from vendor in order to set up in PeopleSoft.</p> <p>The AP employees entering voucher information do not print checks.</p> <p>Printed checks are reviewed for payments to employees.</p> <p>Payments are authorized by department authorized signers responsible for spending of department funds.</p> | | |
| 7 | Checks are received by the appropriate vendor | <ol style="list-style-type: none"> 1. Checks are lost or stolen in process of being sent to vendor 2. Possible late fees for checks not received. 3. UW's reputation could be damaged | <p>Checks are mailed directly to vendors, which reduces the risk that the checks could be lost on campus.</p> <p>Payment for services provided when the payment occurs at the time of services (speakers) are signed for by the department staff person responsible for paying the individual.</p> <p>Mail pickup occurs daily by mail staff.</p> | <p>Few items are lost in the mail, therefore mailing payments to vendors directly ensures that the checks will be sent off campus to the vendor address of record on a timely basis.</p> | |
| 8 | Payments are requested after the completion/acceptance of the goods or services ordered by the department. | <ol style="list-style-type: none"> 1. Payments are made to vendors without receiving the goods/services. 2. Funds are spent inappropriately. 3. UW's reputation could be damaged. | <p>Checks are paid only when an original invoice from the vendor is included with the information submitted to Financial Services.</p> | <p>Checks are processed only after invoiced and services or goods have been received</p> | |

The University of Wisconsin – Extension
Internal Control Plan – March 2009

| | | | | | |
|----|--|--|---|--|--|
| | | 4. Failure to comply with State, UW System, Board of Regents and institution policies. | <p>Services contracted but not performed are not paid for until performed (no advance payments).</p> <p>An authorized department signor approves the payment of the invoice. This employee is either working in or with the department that receives the goods/services and should know that the goods/services have been received/performed prior to payment.</p> | | |
| 9 | Check stock is safeguarded. | <ol style="list-style-type: none"> 1. Checks could be printed fraudulently. 2. Institution could lose funds | <p>Check stock is unprinted safety paper.</p> <p>A Positive Pay file is sent from PeopleSoft daily to the bank. This file lists the check numbers printed and the amount of payment. Without this information, checks that are presented for payment will not clear our account.</p> | Only those with access to PayCycle will be able to run the process that applies the MICR fonts to the blank check stock that will be accepted by the bank. | |
| 10 | Access to the payment system is secured. | <ol style="list-style-type: none"> 1. Fraudulent payments or vendors could be entered. 2. Institution could lose funds | <p>Access to input payment information is controlled through the use of login IDs and passwords which are assigned by campus staff.</p> <p>Access is given for payment entry only to those staff assigned the responsibility for this process.</p> <p>Access to those who can run PayCycle is limited. Only given to staff who do not have payment or vendor entry authority.</p> <p>Before mailing, printed checks are reviewed by staff that did not enter the payment for odd things such as (payments to staff, large amounts, unusual vendor).</p> | Security is dealt with at the campus level for most access, and can only be overridden at the UW System. Unusual access is reviewed by UW System. | On a monthly basis, Accounting Director runs the PayCycle audit query to validate that the same employee did not enter and run PayCycle for the same vouchers. |

E-3 Control Matrix – General Ledger Entries

| NO. | INTERNAL CONTROL | RISKS | KEY CONTROL POINTS | | |
|-----|--|---|---|--|--|
| | | | Operating Controls | Monitoring Controls | Oversight Controls |
| | Listed below are the sub-processes within the overall Journal Entry process and what we are trying to control for within this sub-function. | This column lists risks inherent to the process which might cause inaccurate data or inaccurate activity. | | | |
| 1 | Ensure there is a clear process to determine who is authorized to process J.E.s, who is authorized to approve J.E.s and who grants that authority. | <ol style="list-style-type: none"> 1. Unauthorized individuals processing J.E.s 2. Improper/inappropriate charges to chartfields 3. Non-compliance with governmental regulations 4. Inaccurate financial statements 5. Fraud | <p>Within unit, have clear definition of who is authorized to grant the ability to process J.E.s and grant the ability to approve J.E.s</p> <p>Shared Financial System (SFS) User Request Authorization Form should be completed and approved to grant or cancel/revoke access to SFS in order to process J.E.s</p> | Monitor activity to ensure all J.E.s were processed and approved by only authorized individuals | Review the Data Security Report to validate that all individuals with access to process J.E.s is appropriate |
| 2 | All authorized operators and approvers of J.E.s should receive proper training prior to entering/approving J.E.s into the system. | <ol style="list-style-type: none"> 1. J.E.s are processed incorrectly 2. Improper/inappropriate charges to projects/funds 3. Non-compliance with governmental regulations 4. Inaccurate financial statements 5. Fraud | Provide training to employees using the UWSA SFS User guide and Training Manual | Monitor activity to ensure all J.E.s were processed by only properly trained individuals | Review the Data Security Report to validate that all individuals with access to process J.E.s is appropriate |
| 3 | Ensure J.E. is prepared accurately, is complete and is valid | <ol style="list-style-type: none"> 1. J.E.s are processed incorrectly 2. Improper/inappropriate charges to projects/funds 3. Non-compliance with governmental regulations 4. Inaccurate financial statements 5. Fraud | Ensure clear and complete, self-explanatory descriptions are provided in the header's long descriptor field and line description fields and all other input has been correctly completed including amount and chartfield allocation. | Perform Edit and Budget checks of chartfields upon completion (or will be done overnight automatically). | |
| 4 | Every J.E. should be reviewed and approved by the appropriate individual to ensure it is accurate and appropriate | <ol style="list-style-type: none"> 1. J.E.s are processed incorrectly 2. Improper/inappropriate charges to projects/funds 3. Non-compliance with governmental regulations 4. Inaccurate financial statements | J.E.s should be reviewed and approved by someone who is in a higher level position of authority to confirm that the J.E. is appropriate, accurate, complies with appropriate policies and is properly explained | Monitor activity to ensure all J.E.s were approved by individuals on the Authorized Signer list. | |

The University of Wisconsin – Extension
Internal Control Plan – March 2009

| | | | | | |
|---|---|--|--|--|--|
| | | 5. Fraud | and documented. J.E.'s require the signature of the preparer, Division and Business Services. | | |
| 5 | Ensure the appropriate back-up and support for non-sponsored J.E.s is available and provided if necessary | <ol style="list-style-type: none"> 1. Inappropriate/non-supportable J.E.s 2. Improper/inappropriate charges to projects/funds 3. Non-compliance with governmental regulations 4. Inaccurate financial statements | <p>J.E. should stand on it's own / be self-explanatory. Back-up should be provided.</p> <p>Business Services reviews for reasonableness.</p> | | |
| 6 | Ensure proper back-up support is provided for J.E.'s affecting Sponsored Programs | <p>Non-compliance with governmental or non-governmental funding agency regulations</p> <p>Potential disallowance of costs by funding agency.</p> | <p>Department and Division are responsible for preparing transfers in accordance with the terms and conditions of their extramural support award.</p> <p>Office of Extramural Support (OES) must approve all J.E.s affecting all sponsored activity, and only do so upon reviewing the appropriate back-up. OES will notify originating unit and provide comments for any changes they make to any J.E.s</p> | | |

E-4 Control Matrix – Purchasing Card (P-Card)

| NO. | INTERNAL CONTROL | RISKS | KEY CONTROL POINTS | | |
|-----|--|---|---|---|---|
| | | | Operating Controls | Monitoring Controls | Oversight Controls |
| | Listed below are the sub-processes within the overall P-Card Procurement process and what we are trying to control for within this sub-function. | This column lists risks inherent to the process which might cause inaccurate data or inaccurate activity. | | | |
| 1 | Ensure there is a clear process to determine who is authorized to possess a P-Card and who has the authority to make that decision. | Unauthorized individuals possessing P-Cards Misappropriation of funds Unnecessary or inappropriate purchases | Units may establish local guidelines for P-Card holder criteria stricter than University guidelines. If local policies are in place, business practices would be needed to ensure applicants meet local criteria. Written procedures clearly outline who is authorized to possess a P-Card, who is authorized to be a P-Card approver, and details of other unit P-Card procedures such as receiving, approvals and reconciliations. | An employee's supervisor and the Unit Business Representative maintains the discretion to determine if a purchasing card is needed. | Business Services (BS) monitors all P-Card applications to ensure that the cardholders are regular University employees (cannot be students or LTE's) |
| 2 | Ensure there is a clear process to determine who is authorized to be a P-Card approver and who has the authority to make that decision. | Misappropriation of funds Overpayment Unnecessary or inappropriate purchases | Individuals cannot approve their own P-Card statements or their own expenses on another cardholder's statement | Divisions have the authority to approve applications, and the cardholder's liaison is responsible for reviewing activity against each month's billing statement. | BS verifies that the applicants signed the application. |
| 3 | All authorized P-Card holders and approvers should receive proper training prior to taking possession of a P-Card or approving P-Card transactions | Purchases are made incorrectly Overpayment Unnecessary or inappropriate purchases Potential conflict of interest? Fraud | There is mandatory training for the cardholder and liaison before the card is issued. They are also directed to read the P-Card Manual before the card is issued. | The cardholders' acknowledgement that they read and understand the requirements. | Business Services will not issue the card until the training is completed. |
| 4 | Ensure the P-Card application is completed correctly. | Unauthorized individuals possessing P-Cards Misappropriation of funds Unnecessary or inappropriate cash and credit limits | Cardholder is responsible for completing the application. | P-Card approver reviews and approves applications to ensure they are the appropriate approver, the reconciler is appropriate and credit limits are in line with the needs of the cardholder and the unit, and the application is consistent with local policies where applicable. | BS verifies that the application has been signed by the employee, supervisor, and Unit Business Representative (or designate). BS reviews the application and ensures the applicant is currently an employee (and not a student or LTE), the account strings are entered correctly, and that contact information has |

The University of Wisconsin – Extension
Internal Control Plan – March 2009

| | | | | | |
|---|---|--|---|---|---|
| | | | | | been provided. |
| 5 | Ensure the use of the card is appropriate and consistent with University guidelines | <p>Misappropriation of funds</p> <p>Overpayment</p> <p>Unnecessary or inappropriate purchases</p> <p>Improper/inappropriate charges to projects/funds</p> <p>Non-compliance with Federal laws and guidelines</p> <p>Potential conflict of interest</p> | Cardholder is responsible for using the purchasing card in a manner consistent with the requirements. The cardholder is required to be knowledgeable of the requirements in the UW-Extension P-Card Manual. | <p>Approver should review cardholder purchases to ensure purchases are:</p> <ul style="list-style-type: none"> • authorized, appropriate and reasonable • for business use only • less than \$5,000 each • not entering into a Conflict of Interest • consistent with budget/project/grant guidelines • not split orders • not restricted items • made by the cardholder and not someone else • consistent with University guidelines • exempt from sales tax where appropriate <p>Any suspicious activity is reported.</p> | <p>BS provides Unit Business Representatives and cardholders with access to the US Bank Access Online application, which includes various reports and information.</p> <p>BS reviews transaction reports on a bi-weekly basis and may follow-up on the appropriateness of a given item.</p> <p>BS staff does a complete post audit of all purchasing card charges made by UWEX cardholders.</p> |
| 6 | Make sure the P-Card is the appropriate buying mechanism for purchases | <p>Overpayment</p> <p>Non-compliance with Federal standards</p> <p>Misappropriation of funds</p> <p>Inefficient processing cost and lower supplier performance</p> | Cardholder is responsible for using the purchasing card in a manner consistent with the requirements. | Approver should monitor cardholder purchases to ensure P-Card was the appropriate buying mechanism and other methods such as Internal Service Units, University Contracts, or Purchase Orders would not have been appropriate. | BS periodically reviews transactions and may follow-up on the appropriateness of a given item. BS staff provides Unit Business Representatives access to the US Bank Access Online application, which includes various reports and information. |
| 7 | Ensure goods are received and there is proper follow-up with suppliers to resolve any discrepancies | <p>Overpayment</p> <p>Payment for goods/services not received</p> <p>Payment for damaged goods</p> <p>Fraud</p> | The cardholder is responsible for this task. Cardholder calls vendor about product not received or to solve any discrepancies. If the problem is not resolved by calling the vendor, the cardholder calls US Bank to file an official dispute notice. | Approver should ensure cardholder has received all goods/services purchased and notified the vendor of any discrepancies | If BS receives an invoice from a vendor that appears to have been already paid with a purchasing card, the invoice is not paid and it is sent to the department. |
| 8 | Assign proper codes and descriptions to all transactions | <p>Improper/inappropriate charges to projects/funds</p> <p>Non-compliance with Federal standards</p> <p>Inaccurate financial statements</p> <p>Fraud</p> | Either the cardholder or the reconciler should make sure all purchases are assigned to the proper codes. | Approver should review the assigned codes to ensure they are appropriate. | <p>BS discourages the use of default coding. Appropriate codes should be entered on a line-by-line basis.</p> <p>BS can make adjustments to the account coding strings if necessary.</p> |

The University of Wisconsin – Extension
Internal Control Plan – March 2009

| | | | | | |
|----|--|--|--|--|--|
| 9 | Ensure the reconciled P-Card statement, receipts and other documentation are submitted and approved on a timely basis | <p>Misappropriation of funds</p> <p>Overpayment</p> <p>Unnecessary or inappropriate purchases</p> <p>Improper/inappropriate charges to projects/funds</p> <p>Non-compliance with Federal standards</p> | <p>Cardholder is responsible to sign the reconciled P-Card Statement, submit along with the supporting documents to the approver in time to allow the approver sufficient time to review and approve.</p> <p>Individuals should not be approving their own P-Card statements</p> | <p>The liaison reviews the log form and back-up documentation immediately after the billing cycle ends. Specific controls may vary by department. Overall, areas of focus should include that the approver (liaison) ensures the appropriate supporting documentation is provided for each transaction and the form is reconciled correctly. The approver should sign each monthly P-Card Statement for their assigned cardholders endorsing that the charges are legitimate, reasonable and appropriate. All incomplete or incorrect items should be returned to the cardholder for correction. The approver should request reimbursement for any inappropriate items.</p> <p>Any suspicious activity should be reported.</p> | BS staff does a post audit to make sure all receipts and back-up materials are attached to statements. |
| 10 | Ensure all charges and credits on the Statement of Activity are reconciled and all errors are resolved on a timely basis | <p>Misappropriation of funds</p> <p>Overpayment</p> <p>Unnecessary or inappropriate purchases</p> <p>Improper/inappropriate charges to projects/funds</p> <p>Non-compliance with Federal standards</p> | Cardholder reconciles, and liaison reviews, all charges and credits. | Reconcile all P-Card activity on the Statement of Activity to backup detail to ensure purchases have been assigned to proper codes and designated accounts are appropriate. Contact cardholder/vendor of any discrepancies. | Cardholders and liaisons receive up to three emails from P-card Administrator reminding them to allocate the charges. If the charges are not allocated within the time frame, the charge is assigned a supply account code and default coding is used. |
| 11 | Ensure all change requests to cardholder profile, credit limits, and approver or reconciler are submitted and approved appropriately | <p>Misappropriation of funds</p> <p>Unnecessary or inappropriate cash and credit limits</p> | All change requests are reviewed and approved by Business Services. | P-Card approver should review and approve all change requests to ensure the approver and reconciler are appropriate, and credit limits are in line with the needs of the cardholder. | Business Services reviews changes on US Bank Access Online |

The University of Wisconsin – Extension
Internal Control Plan – March 2009

| | | | | | |
|----|---|--|--|---|---|
| 12 | Notify Business Services to deactivate P-Cards for all employees leaving the department/unit or University | <p>Misappropriation of funds</p> <p>Overpayment</p> <p>Unnecessary or inappropriate purchases</p> <p>Improper/inappropriate charges to projects/funds</p> <p>Non-compliance with Federal standards</p> | <p>Cardholder, liaison, or Division should notify Business Services or submit a P-Card Maintenance form immediately upon awareness or notice of departure to deactivate P-Cards for any employees leaving the unit or University, but no later than the termination date.</p> <p>The cards should be collected and shredded.</p> | | <p>Every month BS receives a termination list from UWEX Payroll. BS reviews this list immediately for employees who have P-Cards or are liaisons. The P-Card is immediately deactivated (if not already deactivated).</p> |
| 13 | Contact P-Card vendor upon discovery that P-card is lost or stolen or fraudulent charges are discovered on the account. | Misappropriation of funds | Cardholder should contact the P-Card vendor immediately upon discovery to report a lost or stolen card or any fraudulent activity. | Cardholder and liaison monitor P-Card statement to ensure no charges have been processed after the card has been cancelled. | |

E-5 Control Matrix – Cash Handling (Cash, Check, Money Order, Traveler’s Check, Credit Card)

| NO. | INTERNAL CONTROL | RISKS | KEY CONTROL POINTS | | |
|-----|--|--|---|--|--|
| | | | Operating Controls | Monitoring Controls | Oversight Controls |
| | Listed below are the sub-processes within the overall P-Card Procurement process and what we are trying to control for within this sub-function. | This column lists risks inherent to the process which might cause inaccurate data or inaccurate activity. | | | |
| | Basic Requirements | | | | |
| 1 | Statutory Requirements - Comply with Wisconsin State Statute 20.906 | Penalty for noncompliance. Risk of theft or embezzlement with large sum of cash on the premises Weak cash management control | Deposit in or transmitted to the State treasury at least once a week. Deposit daily or more frequently than once a week if more than \$100.00 daily or whenever on hand revenue exceeds \$300.00. | Communicate to staff who handle cash that internal cash control is a priority | Communicate to all members of the organization who handle cash that internal cash control is a priority |
| 2 | Physical control | Risk of lost resulted from cash stored in container that is not specified for keeping cash. Risk of lost resulted from using inappropriate storage for the container holding the cash Risk of temptation resulted from easy access (or common knowledge) to the keys to the cash container/cash storage facility | Store money collected in the most secure facilities available, preferably a safe or vault. Secure cash boxes into a locked file cabinet, desk drawer, or closet, if needed. The custodian will lock up or secure the cash at all times. Never leave money unattended. Department is responsible for security of revenue. Report any burglary or theft to UW Police and Risk Management as soon as discovered. Safeguard revenue by following revenue handling procedures. | Assign responsibility for monies collected to one (as designed fund custodian) or two (as alternate custodian) staff persons within the department. Hold to a minimum the number of individuals with keys to cash boxes or safe combinations. Inventoried on a list with the name of the custodian and date assigned. Locks and safe combinations should be changed every two years and when employees terminate. | Provide and Assign Appropriate Physical Storage Devices. Ensure the tightest security measures possible are implemented. Restrict access to places of safekeeping, such as safes and cash boxes, to those responsible for monies collected. Internal auditor examines all areas where funds might be maintained to make sure funds are secured. |
| 3 | Transit control | Moving cash by one staff may post hazard. Threat of external theft or robbery. | Cash picked up by armored car service from department to Bank. Verify cash received when brought to Cashier's office for deposit. | Develop cash handling procedures. | Internal auditor examines transit procedures to make sure funds are secured and staff are safe. |
| 4 | Collection control - cash | Cash fraud and abuse Stolen or misappropriation of cash Inaccurate accounting Create opportunity for temptation that could lead to cash fraud. | Verify currency in a designated area away from public access. Require proper identification and proof of authorization if someone requests access to records, or wants to count money in your possession. | Develop cash handling procedures. Review bank reconciliation thoroughly and independently. Reconcile receipts with WISDM. | Surprise cash count by Internal Auditor or Controller to verify fund on hand. Determine appropriate separation of duties and supervisory review of cash management activities. |

The University of Wisconsin – Extension
Internal Control Plan – March 2009

| | | | | | |
|---|--|---|---|---|--|
| | | <p>Cash transactions not documented or recorded immediately leads to an opportunity for errors.</p> <p>Temptation</p> <p>Unethical cash practices</p> | <p>Cash counts must be performed in the presence of the person responsible for the cash.</p> <p>Use pre-numbered receipt books for any transaction involving currency.</p> <p>DO NOT make refunds from cash on hand.</p> <p>Cash receipts are not to be withheld from deposit to establish a change fund nor should personal funds be used.</p> | <p>Analyze all written receipts for incoming cash to ensure that they were recorded on a deposit slip and, subsequently, on the bank statement.</p> | |
| 5 | <p>Collection control – credit card (See Annex E-12 and E-13 for additional controls.)</p> | <p>Stolen or misappropriation of credit card information</p> <p>Human error</p> | <p>Accept credit card payment for the amount owed only.</p> <p>Safeguard credit card slips.</p> | <p>Confirm that no personal credit card substituted for receipts</p> | <p>Determine appropriate separation of duties and supervisory review of cash management activities.</p> |
| 6 | <p>Collection control – checks, money orders, traveler's check</p> | <p>Stolen or misappropriation of fund</p> <p>Inaccurate accounting</p> <p>Fraud.</p> <p>Human error</p> <p>Temptation</p> <p>Unethical cash practices</p> | <p>Accept checks for the amount owed only.</p> <p>Do not accept post dated checks or two party checks</p> <p>Endorse all checks, postal money orders, and travelers checks immediately upon receipt, using department's "For Deposit Only" endorser, to make the checks non-negotiable if stolen.</p> <p>Examine checks to make sure they are complete and accurate:</p> <ul style="list-style-type: none"> • made payable to the University • digit amount and the written amount must be the same <p>signed. Travelers checks must be signed in two places.</p> | <p>Confirm that no un-receipted checks substituted for cash deposits</p> <p>Assign responsibility of cash receipt, cash deposit and reconciliation be performed by different staff persons.</p> <p>Review WISDM thoroughly and independently.</p> <p>Reconcile receipts with WISDM.</p> <p>Verify the breakdown of cash and checks per the receipts matched the breakdown of cash and checks recorded on the deposit slips.</p> | <p>Examine all areas where funds might be maintained to make sure funds are secured.</p> <p>Determine appropriate separation of duties and supervisory review of cash management activities.</p> |
| 7 | <p>NSF checks</p> | <p>Unethical cash practices</p> <p>Human errors</p> <p>Improper records</p> | <p>Follow NSF collection procedures established in Cashier's office.</p> <p>Prepare bad check list</p> <p>Do not accept personal check from a person with history of NSF checks as payment on a NSF check</p> <p>Charge NSF fee per Wis Statutes.</p> <p>Do not make a refund to someone on the bad check list.</p> | <p>Develop NSF procedures.</p> <p>Review the bad check list to determine if update is needed</p> <p>Make sure fees charged for NSF are accounted for.</p> <p>Assign responsibility for refund approval and refund issuance to two different staff persons.</p> | <p>Determine appropriate separation of duties and supervisory review of cash management activities.</p> |

The University of Wisconsin – Extension
Internal Control Plan – March 2009

| | | | | | |
|----|--|--|---|--|---|
| 8 | Deposit - Ensure there is a clear process to determine who is authorized to handle cash and follow uniform deposit procedures. | <p>Fraud not detected</p> <p>Human errors</p> <p>Improper records</p> <p>Unethical cash practices</p> | <p>Follow established deposit procedures.</p> <p>Deliver all revenue to UWEX Cashier Services along with proper documentation within 5 days of receipt so that deposit can be made within one week in compliance with Wis. State Statute.</p> <p>Avoid having large amounts of revenue on hand over the weekend or holidays.</p> <p>Make daily deposits if daily receipts exceed \$100.00 and anytime on-hand receipts exceed \$300.00.</p> <p>No sizable amount of currency should accumulate.</p> <p>Never use campus mail to send currency for deposit. Currency must be hand delivered to the Cashier's office and verified by both the cashier and the person delivering the currency.</p> | <p>Establish deposit procedures.</p> <p>Assign the responsibility for collection, deposit, and reconciliation of revenues to different individuals.</p> <p>Maintain proper records, including receipt and deposit records backup, inventories of saleable items, reconciliation of deposit, etc.</p> <p>Review deposits quarterly to determine that funds were deposited as required and amounts were posted to the proper General Ledger account.</p> <p>Analyze the deposit mix – cash, checks, credit cards</p> | <p>The degree of separation of duties would depend on the revenue activity and the number of staff in the department.</p> <p>Random reviews of deposits, reconciliations, and other documentation to establish that procedures are being followed and revenues and expenditures are reasonable.</p> |
| 9 | Over and short | <p>Fraud not detected</p> <p>Human errors</p> <p>Improper records</p> <p>Unethical cash practices</p> | <p>Follow over and short handling and follow-up policy and procedures.</p> <p>Maintain an over and short log.</p> <p>Document on resolution.</p> | <p>Review over and short log periodically to determine if there is a pattern.</p> <p>Review over and short log periodically to determine reasonableness on resolution.</p> | <p>Process in place for timely correction of errors and detection of fraud.</p> |
| 10 | Petty cash | <p>Use of fund for personal purchases.</p> <p>Fraud</p> <p>Human error</p> <p>Temptation</p> <p>Fail to anticipate cash needs for business related purchases</p> <p>Unethical cash practices</p> | <p>Follow Revenue Handling Procedures.</p> <p>Maintain a petty cash log and receipts to account for related transactions.</p> <p>May only be used for minor expenses specified in the Cash Fund Advance Agreement.</p> <p>No purchase in excess of \$50.00 may be made from the fund.</p> <p>Must be reimbursed periodically and at the end of the fiscal year by submitting original receipts or</p> | <p>Verify cash and purchase receipts totaling the fund issued.</p> <p>Reconcile at least weekly, and daily if for more than \$100.00.</p> <p>Verify purchases only for items normally allowable under University Purchasing Rules.</p> <p>Review accounting reports and cash flow statements.</p> | <p>Process in place for timely correction of errors and detection of fraud</p> |

The University of Wisconsin – Extension
Internal Control Plan – March 2009

| | | | | | |
|----|--|--|---|---|--|
| | | | documentation with a Travel Expense Report through regular channels. Security over a cash fund is the personal responsibility of the fund custodian. | | |
| 11 | Change fund | Use of fund for personal purchases or other non-business purpose. Human error Temptation Unethical cash practices | Used only for making change for sales transactions. Not to be used for cashing personal checks, as a petty cash fund, or for any other non-business purpose. | Verify the amount on hand not less than the amount of the change fund authorized on the Cash Fund Advance Agreement. | Process in place for timely correction of errors and detection of fraud |
| | Depositing Revenue | | | | |
| 12 | Revenues – program revenues or fee directly related to the cost of goods/services. | Revenues received were not properly accounted for due to fraud and error. Unethical cash practices | Use “Report of Registrations and Collections” (RRC) form to detail the deposit and accounting entry such as program title, fund acct rev, list all enrollees and their check numbers. No collected Revenues are to be used to offset expenses, make refunds, or establish a change or petty cash fund. All receipts are forwarded to the UWEX Cashiers Office for deposit, along with 2 copies of the RRC. Computations checked for accuracy: <ul style="list-style-type: none"> • Double check all addition on the RRC • Include an adding machine tape of the checks and cash to show that the amount of revenue equals the paper documentation. Retain a copy of the RRC for department’s records then compare with the receipt copy from Cashiers. | Program revenues should be set up during the budget process, based on a specific level of anticipated revenue. Make sure deposits are made intact. Review cash management activities and adequate segregation of duties exist. Establishment of internal and external communication channels to report errors and suspicious of improprieties. | Review budget and actual for reasonableness. Process in place for timely correction of errors and detection of fraud. Determine appropriate separation of duties and supervisory review of cash management activities Review override or variances for reasonableness. Internal audit of revenues. |
| | Refunds | | | | |
| 13 | Refunding revenue collected | Unethical cash practices | Department is responsible for determining whether the refund is due per their department’s policies and program brochures. They are also responsible for retaining backup on each refund for seven years for audit purposes. | Ensure the person responsible for depositing revenue not the same person approving the refund request. Separation of these duties should be followed Review cash management | Process in place for timely correction of errors and detection of fraud. Determine appropriate separation of duties and supervisory review of cash |

The University of Wisconsin – Extension
 Internal Control Plan – March 2009

| | | | | | |
|--|--|--|---|---|------------------------------|
| | | | <p>All refunds must be requested through the Cashier Services and a University of Wisconsin check issued by filling out refund request cards. No refunds from revenue on hand allowed.</p> <p>Refund checks are mailed out by the Accounts Payable Office</p> | <p>activities and adequate segregation of duties exist.</p> <p>Establishment of internal and external communication channels to report errors and suspicious of improprieties</p> | <p>management activities</p> |
|--|--|--|---|---|------------------------------|

E-6 Control Matrix – Capital Assets

| NO. | INTERNAL CONTROL | RISKS | KEY CONTROL POINTS | | |
|-----|--|--|---|---------------------|--|
| | | | Operating Controls | Monitoring Controls | Oversight Controls |
| | Listed below are the sub-processes within the capital equipment process and what we are trying to control for within this sub-function. | This column lists risks inherent to the process which might cause inaccurate data or inaccurate activity. | | | |
| 1 | Recorded capital asset acquisitions represent capital assets acquired by the organization. Every capital asset is assigned a capital asset number and is physically tagged. | Assets recorded in the capital Inventory System may be fictitious. All capital assets may not be appropriately accounted for. | The Capital Asset BS Staff is responsible for updating the capital Inventory System for new acquisitions on a monthly basis. SFS is queried for all charges to capital account codes during the month to ensure every capital asset is assigned a number and added to the inventory system. On a quarterly basis BS staff add DFD funded acquisitions to the inventory system. | | On an annual basis, DFD acquisitions and SFS additions are reconciled by BS to the amount reported to UWSA for GAAP financial reporting. |
| 2 | The Purchasing Department is involved in the purchase of capital assets. | Adequate guidance and oversight may not have been provided in the acquisition process. | Purchasing is actively involved with assisting departments with the paperwork required for acquisitions, including facilitating the bidding process. | | |
| 3 | Prior to the acquisition of any capital asset, a capital authorization is obtained. | Assets acquired may not have been appropriately authorized. Adequate guidance and oversight may not have been provided in the acquisition process. The asset acquired may not have represented the best value or best quality among the available options. | UW Extension follows the State's guidelines regarding conducting a bid or sealed bid process. DOA sets the thresholds by which bids must be obtained (\$5,000), as well as where sealed bids must be obtained (\$25,000), as well as the procedures for obtaining a waiver from the bidding process. The threshold for capitalizing an asset and performing the bid process (\$5,000) are consistent, which ensures that the appropriate authorizations have been provided. | | |
| 4 | Capital expenditures that were incurred outside of the established protocol described in #4 are identified and addressed. | Assets acquired may not have been appropriately authorized. | Purchasing sends an illegal purchase notice letter to the department who acquired the asset and informs them of the need to go through the bid (whichever is applicable) process. In general, Purchasing does not require that the transaction be negated, unless they are informed of the | | |

The University of Wisconsin – Extension
Internal Control Plan – March 2009

| | | | | | |
|---|---|---|---|--|--|
| | | | purchase before the asset has been received. | | |
| 5 | Capital expenditure overruns are anticipated and properly approved. | Acquisition costs may not be adequately monitored and controlled. | Capital asset expenditure overruns are most likely to occur on construction contracts. The State Building Commission assigns a project manager for construction projects (both where State and where UW Extension funds are used), and this person is responsible for anticipating and approving overruns, as well as making any necessary adjustments to accommodate overruns. | | . |
| 6 | Depreciation methods are established by UWSA | The correct value of a capital asset may not be getting captured for financial reporting purposes. The correct depreciation method may not be getting applied; depreciation may not be getting calculated correctly. Depreciation expense may be misstated. | N/A for UW-Extension. Since SFS is on a cash basis, accumulated depreciation/depreciation expense is not recorded in the ACTUAL ledger. It is taken into account by UW System Administration in the FINRPT ledger at the time the financial statements are generated. UWSA uses a straight-line depreciation method and assigns useful lives based on the type of equipment. | | Accumulated depreciation and depreciation expense is calculated annually by BS and reported to UWSA for GAAP financial reports. |
| 7 | All capital asset disposals are recorded. Recorded capital asset disposals represent actual disposals. | Capital asset records are inaccurate. May be an indicator that disposal policies and procedures were not followed. Risk of misappropriation of assets may increase. | Responsibility for ensuring a disposal is an actual disposal is with the department who is custodian of the asset. The Capital Asset BS staff is responsible for updating the capital assets Inventory System for disposals that have been communicated to BS. | | BS reviews total disposals for year-end GAAP reporting to UWSA. BS completes a physical inventory every odd numbered fiscal year per UW System policy. This inventory ensures the existence of items on the inventory system. |
| 8 | Capital asset can only be taken off inventory system by Property Disposition Report form or Surplus Property Pick-up Request form, is completed by department and approved by the Purchasing Department. Purchasing Department faxes Surplus Property Pick-up Request form to SWAP and capital assets are removed from Inventory System. Capital Assets on the Property Disposition Report are removed | Disposals may not be appropriately authorized; increased potential for fraud, waste, and abuse. | UW Extension has established a process to meet this control objective. Departments are responsible for filling out this form and sending it to the Purchasing Department. | | |

The University of Wisconsin – Extension
Internal Control Plan – March 2009

| | | | | | |
|----|--|--|---|--|--|
| | from Capital Inventory System or assigned new user information (in a transfer) after Purchasing Department approval. | | | | |
| 9 | Fixed assets are adequately safeguarded. | Misappropriation of assets and/or vandalism may occur. | Security is the responsibility of the department who is the asset custodian. The level of security provided depends on the nature of the asset. Security provided for an asset is not reviewed during the inventory process. | | |
| 10 | BS staff completes and submits the summary of changes in capital inventory to UW System Administration for financial reporting purposes. | Inaccurate financial reporting, including recognition of depreciation expense. Misappropriation of assets; assets acquired without necessary authorization. | BS staff reviews a report produced by IT Department of all Adds and Deletes to the Inventory System. This report is checked against the SFS monthly reports for adds and Property Disposition/Surplus Property Forms for deletes. | | Depreciation is calculated annually only for financial reporting purposes. |
| 11 | A physical inventory of capital assets is taken periodically and reconciled to the Inventory System. | Misappropriation of assets; inaccurate financial records. | BS completes a physical inventory every odd numbered fiscal year per UW System policy. | | |

E-7 Control Matrix – Fraud Detection

| NO. | INTERNAL CONTROL | RISKS | KEY CONTROL POINTS | | |
|-----|---|---|--|--|---|
| | | | Operating Controls | Monitoring Controls | Oversight Controls |
| | Listed below are the sub-processes within the overall Fraud Prevention process and what we are trying to control for within this sub-function. | This column lists risks inherent to the process which might cause inaccurate data or inaccurate activity. | | | |
| | Occupational Fraud & Abuse | | | | |
| 1 | <p>Assets Appropriations</p> <p>Protect assets from scheme that involves the theft or misuse of an organization's assets.</p> <p>Place a high priority on integrity and be free of any unnecessary pressures. The result is the addition of effective internal monitoring to process controls, and the alignment of the employees with the goals of the organization.</p> | <p>Fraudulent invoicing/disbursements</p> <p>Payroll fraud</p> <p>Skimming revenues</p> <p>Motivation arises from personal financial obligations or conflicting relationships between employees and the organization.</p> | <p>Hire and retain honest people.</p> <p>Conduct background check</p> <p>Segregation of duties.</p> <p>Make sure that all employees who have custody of assets or are responsible for sensitive record keeping or authorization functions take an annual vacation. Periodic rotation of duties among key employees can achieve similar results.</p> | <p>Ensure employees understand the important of integrity and honesty.</p> <p>All dishonest acts should be investigated, and the guilty should be prosecuted and dismissed immediately.</p> <p>Minimize opportunity.</p> <p>Resolve all conflicts promptly.</p> | <p>Encourage an atmosphere based on honesty from the top down — as well as adopting and ensuring compliance to a strict code of conduct.</p> <p>Establish clear rules for conduct and specify the sanctions.</p> <p>Removed unsavory employees immediately from sensitive jobs and denied access to the computer to prevent them from seeking retribution by damaging the system.</p> |
| | Cash Misappropriations | | | | |
| 2 | <p>Detect Skimming</p> <p>Detect acts of removal of cash prior to its entry into the accounting system.</p> | <p>Employee accepts payment from a vendor but does not record the revenues.</p> <p>Revenues falling due to employee pocketing money.</p> <p>Revenues and cash not reconciled.</p> <p>Cash and inventory not reconciled.</p> | <p>Watch for unusual behavior or work habit of your co-workers.</p> <p>Install surveillance equipment at registers or other places where large amount of cash is accepted.</p> <p>More than one employee observe cash count simultaneously</p> <p>Require receipt for all cash transactions. Use pre-numbered receipt book.</p> <p>Do not use cash receipts for expenses or cash check.</p> <p>Practice a good accounting.</p> | <p>Increase management presence by stopping by areas where cash is received several times during the day help deters theft.</p> <p>Conduct surprise cash counts.</p> <p>Limit number of employees handling cash registers or void register transactions. Unique login ID for employee.</p> <p>Examine the mix of credit cards, checks and currency and do an analysis of the deposit.</p> <p>Follow-up if there was a decreasing ratio of cash to credit card sales.</p> | <p>Establish Fraud Hotline or encourage employee to call Fraud Hotline established by LAB: 1-877-FRAUD-17.</p> <p>Contact FBI and/or local police if needed.</p> <p>Notify IRS of possible tax fraud</p> |

The University of Wisconsin – Extension
Internal Control Plan – March 2009

| | | | | | |
|---|--|---|---|--|--|
| | | | | <p>Follow-up on flat or declining sales with increasing cost of sales or missing inventory.</p> <p>Follow-up if there was an increasing accounts receivable compared with cash.</p> <p>Follow-up if delayed in posting of accounts-receivable payments.</p> | |
| 3 | <p>Detect Cash larceny</p> <p>Safeguard cash from being removed from the organization after it has been entered into the accounting records.</p> | <p>Employee steals currency from daily receipts before they can be deposited in the bank.</p> <p>Increase in accounts receivable.</p> <p>Discrepancy between the accounts receivable detail and cash.</p> <p>Alter the deposit slips.</p> | <p>Watch for unusual behavior or work habit of your co-workers.</p> <p>Make sure deposits preparation is within the scope of the job description of the backup personnel.</p> | <p>Examine the mix of credit cards, checks and currency and do an analysis of the deposit. If someone is stealing currency, it usually will show up in an analysis of the deposits and bank reconciliations and cash counts.</p> <p>Follow-up on unexplained cash discrepancies.</p> <p>Follow-up on altered or forged deposit slips.</p> <p>Follow-up on customer complaint about billing and payment.</p> <p>Determine the cause of rising "in transit" deposits during bank reconciliations.</p> <p>A periodic review of receipts and disbursements</p> <p>Make sure that the deposits are made intact.</p> | <p>Establish Fraud Hotline or encourage employee to call Fraud Hotline established by LAB: 1-877-FRAUD-17.</p> <p>Contact FBI and/or local police if needed.</p> <p>Notify IRS of possible tax fraud</p> |
| | Fraudulent Disbursements | | | | |
| 4 | <p>Billings are accurate and truthful.</p> <p>Detect scheme in which a person causes his or her employer to issue a payment by submitting invoices for fictitious goods or services, inflated invoices or invoices for</p> | <p>Employee creates a shell company and bills employer for nonexistent services</p> <p>Employee purchases personal items, submits invoice for payment</p> | <p>Look for checks to unknown vendors or persons</p> <p>Look for checks made out in even amounts</p> <p>Look for dual endorsements</p> <p>Look for checks to cash and to</p> | <p>Use a numbered invoice system.</p> <p>Follow-up on increasing "soft" expenses (for example, consulting or advertising).</p> <p>Follow-up on check to vendor's address that matches employee</p> | <p>Establish Fraud Hotline or encourage employee to call Fraud Hotline established by LAB: 1-877-FRAUD-17.</p> <p>Contact FBI and/or local police if needed.</p> <p>Notify IRS of possible tax fraud</p> |

The University of Wisconsin – Extension
Internal Control Plan – March 2009

| | | | | | |
|---|---|--|--|--|--|
| | personal purchases | | employees. | home address. Follow-up if vendor address is a post office box or mail drop. Vendor name consists of initials or vague business purpose. Excessive voided, missing or destroyed checks. | |
| 5 | <p>Expense reimbursements are truthful.</p> <p>Protect from scheme in which an employee makes a claim for reimbursement of fictitious or inflated business expenses.</p> <p>Detect when employee files fraudulent expense report, claiming personal travel, nonexistent meals, altered document, etc.</p> | <p>Mischaracterization of expenses – Employees submitted legitimate documentation for non business-related transactions. Example: taking a friend to dinner and charging it to the company as "business development", or "consultation" or "interview".</p> <p>Overstated expense reports - Employees inflate the amount of actual expenses and keep the difference. Example: altering a taxicab receipt from \$10 to \$40.</p> <p>Fictitious expenses - Employees submit phony documentation for reimbursement. Example: producing a fake hotel bill on a home computer.</p> <p>Improper classification of expenses camouflage the nonreimbursable cost as something for which the employer would pay.</p> <p>Use duplicate or blank receipts or nondescript receipts that camouflage the nature of the expense.</p> <p>Misclassifying personal expenses as work-related.</p> <p>Fabricated expenses that never incurred.</p> <p>Multiple reimbursements - Employees copy invoices and resubmit them for payment more than once. Example: copying an airline ticket and claiming the cost again on next month's expense reimbursement. Or, charge the</p> | <p>Check for irregularities such as multiple receipts from the same source (e.g., taxi company) for the same days, extremely expensive meals, and duplicate meal receipts for the same days and other suspicious charges.</p> <p>Follow-up on receipts that are innocuous-appearing but unknown sources.</p> <p>Examine documentation to make sure expenses were properly characterized, appropriate and authorized</p> <p>Pay close attention to the documentation evidence provided in support of the expense claim to see if it appears to contain alterations, particularly if this is the habit of a single employee, as repeat offenders are the rule, not the exception.</p> <p>Only original documentation is acceptable.</p> <p>No employee allows claiming the expense of another.</p> <p>Verify authorized mileage.</p> <p>When employee signs the TER they are acknowledging that fraud is a criminal offense.</p> <p>Employee's supervisor is responsible for reviewing and signing the TER. The supervisor is verifying that the travel occurred and that the expenses are reasonable.</p> | <p>Expense reimbursements should be monitored periodically by supervisory personnel or auditors. Look for red flags such as increasing expense reimbursements by employee, variations from budgeted expenses and unreasonable charges.</p> <p>Pay reasonable and legitimate expenses.</p> <p>Check out suspicions.</p> <p>Establish expense controls by establishing a limit (e.g., \$500) over which expenses must be submitted for higher up for approval.</p> | <p>Establish Fraud Hotline or encourage employee to call Fraud Hotline established by LAB: 1-877-FRAUD-17.</p> <p>Establish a reasonable reimbursement policy that does not foster dishonest behavior by creating a feeling of resentment that creates other frauds.</p> <p>Contact FBI and/or local police if needed.</p> <p>Notify IRS of possible tax fraud</p> |

The University of Wisconsin – Extension
Internal Control Plan – March 2009

| | | | | | |
|---|---|---|---|---|---|
| | | airline ticket using P-card then submit airline ticket for reimbursement several months later via Travel Expense Report. | | | |
| 6 | <p>Checks are issued for legitimate purposes.</p> <p>Safeguard check tampering – scheme in which a person steals his or her employer's funds by forging or altering a check on one of the organization's bank accounts, or steals a check the organization has legitimately issued to another payee</p> | <p>Breach of a fiduciary duty of care.</p> <p>Employee steals blank checks, makes them out to himself or an accomplice</p> <p>Employee steals outgoing check to a vendor, deposits it into her own bank account</p> <p>Employee forges either the required signature on the face or the payee endorsement on the back of the check</p> <p>Employee obtains and alters a check (usually the payee is altered) so that either the fraudster or an accomplice can misappropriate the check for personal gain</p> <p>Fraudster prepares and submits a fraudulent check, (concealed check schemes) usually in a stack of checks to be signed, during a busy part of the day. The inattentive check signer then signs the check and returns it to the person who prepared it.</p> <p>Someone with check-signing authority who prepares, signs and misappropriates the check for personal gain (authorized maker schemes).</p> | <p>See Annex E-2 for controls in place for checks issues by Business Services.</p> <p>Analyze the accounting records.</p> <p>People who write checks shouldn't be allowed to sign them as it would easily create a false entry in the cash register or simply not make any entry at all.</p> <p>The person reconciling the bank statement should verify that all payees, amounts, dates, signatures and check numbers for all checks processed by the bank match the information contained in the checkbook register.</p> <p>Check signers must carefully and consistently do the following when signing checks:</p> <ul style="list-style-type: none"> • Before signing a check, examine all of the supporting documentation to ensure that the disbursement is for a legitimate business-related purpose. • Make sure that the supporting documentation matches the information written on the check in terms of payee and amount. • The check signer must control the mailing of the check. Never should a signed check be given back to the person who prepared it. <p>Look for odd patterns in the recipients of payments. (e.g., are more checks than usual showing up with second endorsements, or is employee receiving money from the institution if she or he never has before? Most fraud by their nature is</p> | <p>See Annex E-2 for controls in place for checks issues by Business Services.</p> <p>Segregate the responsibilities of preparing checks, signing checks and reconciling the bank statement to the checkbook or disbursement register. If someone has complete control over both the cash receipts and cash disbursements, then have someone review the work.</p> <p>Attentive check signer.</p> <p>Make sure checks are recorded in the check register in a timely fashion. Bank statements are reconciled as they arrive and discrepancies are noted and followed up, and the checking account generally fits into a larger set of financial records.</p> <p>Look for out-of-sequence checks. Look for higher number checks because forged-maker wants to avoid duplicate check numbers. Follow-up if a check has a significantly higher number than the rest of the returned checks in a statement.</p> <p>Control the storage and disposition of signed checks. Checks should be distributed immediately after signing. Handing the checks to the recipients or immediately placing the checks in sealed envelopes after signing and then posting them.</p> <p>Examine front and back of</p> | <p>See Annex E-2 for controls in place for checks issues by Business Services.</p> <p>Establish Fraud Hotline or encourage employee to call Fraud Hotline established by LAB: 1-877-FRAUD-17.</p> <p>Take actions that minimize opportunities to commit fraud and maximize the probability that fraudulent acts will be discovered. Such actions create a "perception of detection," which is the most effective deterrent to fraudulent activity.</p> <p>Contact FBI and/or local police if needed.</p> <p>Notify IRS of possible tax fraud</p> |

The University of Wisconsin – Extension
Internal Control Plan – March 2009

| | | | | | |
|---|--|--|--|--|---|
| | | | something out of the ordinary. | returned checks. Use direct deposit if possible. Protect blank check stock. | |
| 7 | <p>Payroll checks are properly issued.</p> <p>Safeguard from scheme in which an employee causes his or her employer to issue a payment by making false claims for compensation</p> | <p>Employee claims overtime for un-worked hours</p> <p>Employee in Human Resources inputs hours and wages changes the pay rate for the employee.</p> <p>Employee adds ghost employees to the payroll.</p> <p>Forge supervisor's signature on time sheets.</p> <p>Alter time sheets once the supervisor approves them.</p> <p>Supervisors approve timesheets without actually reviewing them.</p> | <p>Attention of informed employee.</p> <p>Watch for unusual behavior or work habit of your co-workers.</p> <p>Supervisor reviews timesheet diligently to make sure that employee did not submit timesheet with more hours than they're entitled to receive or without prior approval from the supervisor.</p> | <p>Segregation of duties concerning employee hiring and payroll. Ideally, these processes should be separated among different people:</p> <ul style="list-style-type: none"> • entering an employee into the payroll system • authorizing pay rate changes • authorizing hours • entering hours worked • distributing the paychecks <p>Periodically check payroll data against approved timesheets.</p> | <p>Establish Fraud Hotline or encourage employee to call Fraud Hotline established by LAB: 1-877-FRAUD-17.</p> <p>Establish rigorous measures to verify the number of hours performed by employees.</p> <p>Contact FBI and/or local police if needed.</p> <p>Notify IRS of possible tax fraud</p> |
| 8 | <p>Accurate register disbursements records.</p> <p>Safeguard scheme in which an employee makes false entries on a cash register to conceal the fraudulent removal of cash</p> | <p>Employee fraudulently voids a sale or receipt or credit on his cash register and steals the cash</p> <p>Employee issues fictitious refunds without return of inventory or documentation.</p> | <p>Attention of informed employee.</p> <p>Watch for unusual behavior or usual purchases of your co-workers.</p> <p>Check for inventory level – the result of cash-register-disbursement frauds push inventory shrinkage to abnormally high levels.</p> <p>Check participants' enrollment sheet. Compare with other conference info such as meals, manuals, etc.</p> <p>Follow-up if cash sales decreasing relative to credit card sales.</p> <p>Follow-up if increasing sales returns and allowances or refunds compared with gross sales or revenues.</p> <p>Watch for altered cash register tapes.</p> <p>Follow-up on increased void or refund transaction by individual employees.</p> | <p>Perform a horizontal analysis – a comparison of financial statement line items from one period to the next to determine if there were odd pattern or unusual growth in line items (e.g., refund)</p> <p>Follow-up on exceptions.</p> <p>Segregation of duties – cashier can not issue refunds without supervision.</p> <p>Follow-up when multiple refunds or voids just under the review limit.</p> | <p>Establish Fraud Hotline or encourage employee to call Fraud Hotline established by LAB: 1-877-FRAUD-17.</p> <p>Develop written Ethics policies and provide anti-fraud training.</p> <p>Contact FBI and/or local police if needed.</p> <p>Notify IRS of possible tax fraud</p> |

The University of Wisconsin – Extension
Internal Control Plan – March 2009

| | Non-cash Assets Misappropriations | | | | |
|----|--|--|--|--|--|
| 9 | <p>Inventory balance is correct.</p> <p>Safeguard against scheme involving the theft or misappropriation of physical, non-cash assets such as inventory, equipment or supplies</p> | <p>Employee steals merchandise from storage room</p> <p>Employee diverts incoming shipments of inventory for personal use</p> <p>Symptoms of Inventory Fraud</p> <ul style="list-style-type: none"> • Missing documents. • Second Endorsements on checks. • Unusual endorsements on checks. • Unexplained adjustments to inventory balance. • Stale items in bank reconciliations. • Old outstanding checks. • Customer complaints. • Unusual patterns in deposits in Transit. • Employees who exceed the scope of their responsibilities. • An unusual reduction in, or less of, a regular customer's business. • Absentee ownership of a small business. • An employee who appears to be living beyond his means. • Open-ended contracts with suppliers. • An unusual increase in purchases by a customer during a brief period. | <p>Attention of informed employee.</p> <p>Watch for unusual behavior or work habit of your co-workers.</p> <p>Ensure products received are entered in inventory account.</p> <p>Seal the boxes in such a manner that the delivery personnel or anyone cannot open it prior to delivery to the client.</p> <p>Keep delivery doors lock at all times. When they are opened for a delivery, they should be under constant supervision by at least two employees.</p> <p>Prepare and maintain a complete equipment list with the description, model and serial number of every article. Keep the equipment list in a secure location.</p> <p>Ensure that inventory is not removed with empty boxes. Empty boxes should be folded and stacked.</p> <p>Follow capital equipment policy and procedures.</p> | <p>Keep an open eye.</p> <p>Periodically count the inventory of stocks without notice and reconcile with inventory accounting records.</p> <p>Follow-up with customer complaints pertaining to invoicing, discounts, or questionable delivery practices</p> <p>Use surveillance system if needed. Affix posters and decals on all equipment.</p> <p>Ensure capital equipment policy and procedures are followed.</p> <p>Determine if write-off or disposition of equipment is reasonable and accurately disposed of.</p> | <p>Establish Fraud Hotline or encourage employee to call Fraud Hotline established by LAB: 1-877-FRAUD-17.</p> <p>Establish capital equipment policy and procedures.</p> <p>Contact FBI and/or local police if needed.</p> <p>Notify IRS of possible tax fraud</p> |
| 10 | <p>Secured Sensitive Information</p> <p>Safeguard scheme in which an employee steals or otherwise misappropriates proprietary confidential information</p> | <p>Employee accesses customer records for purposes of committing identify theft</p> <p>Employee provides confidential information such as company trade secrets to competitor</p> | <p>Watch for unusual behavior or work habit of your co-workers.</p> <p>Call data emergency personnel if data breach is discovered.</p> <p>Failure to adhere to security policy and established procedures may result in disciplinary action.</p> | <p>Access control – all important or confidential papers are kept under lock and key. Limit number of employees have access to information or storage area.</p> <p>Be attentive to hackers accessing computer system.</p> | <p>Establish Fraud Hotline or encourage employee to call Fraud Hotline established by LAB: 1-877-FRAUD-17.</p> <p>Make sure security policy and procedures are established and followed.</p> |

| | | | | | |
|--|--|--|--|--|--|
| | | | | Use password and other security device. Backup information. Develop usage policies for critical employee-facing technologies to define proper use of these technologies for all employees and contractors. | Contact FBI and/or local police if needed. |
|--|--|--|--|--|--|

E-8 Control Matrix – Human Resources – Hiring Practices

| NO. | INTERNAL CONTROL | RISKS | KEY CONTROL POINTS | | |
|-----|---|--|---|---|---|
| | | | Operating Controls | Monitoring Controls | Oversight Controls |
| | Listed below are the sub-processes within the overall Hiring process and what we are trying to control for within this sub-function. | This column lists risks inherent to the process which might cause inaccurate data or inaccurate activity. | Operating Controls | Monitoring Controls | Oversight Controls |
| 1 | <p>Strategic Management (Workforce Needs Determination) -</p> <p>Workforce planning efforts, including performing adequate analyses and developing action plans, to ensure the organization is not left with a serious shortage of qualified workers.</p> <p>Ensure that HR has identified, and is utilizing, suitable recruiting sources that are capable of furnishing adequate numbers of qualified applicants for their organization.</p> | <p>Workforce plan may not meet the organization's strategic mission.</p> <p>Critical skills shortages may not be identified if workforce profiles or gap was not developed or gap analysis was not performed.</p> <p>Failure to project staff requirements may lead to inadequacy in recruitment activities and training and development programs.</p> | <p>A "supply analysis" to provide information on the current workforce profile and what it needs to accomplish future organizational objectives. This analysis would include an employee demographic review and a skill profile.</p> <p>A "demand analysis" provides information on the future workforce needed by the organization.</p> <p>A "gap analysis" compares the current workforce projection and the demand forecast.</p> | <p>Monitor legislative and regulatory environment for proposed changes and the potential impact to the organization and take appropriate steps to support, modify, or oppose proposed changes.</p> <p>Develop action plans to ensure the organization is not left with a serious shortage of qualified workers.</p> <p>Identify and utilize suitable recruiting sources that are capable of furnishing adequate numbers of qualified applicants for their organization.</p> | <p>Conduct ongoing performance assessment of the HR department.</p> <p>Workforce plan linked to the organization's strategic-mission.</p> <p>Determine if the projected staff requirements are used in planning recruitment activities and training and development programs to be offered.</p> <p>Periodically evaluate recruitment sources to ensure that they are meeting the needs of the organization.</p> <p>Review workforce demographics to determine if there is any unusual data trend.</p> |
| 2 | <p>Job Opening -</p> <p>Ensure that candidates have clear information about the qualifications and expectations for the position; ensure that the unit also has a clear understanding of the position and what they need to make a hiring decision</p> | <p>Inappropriate applications; unable to screen and select candidates against weak or missing criteria.</p> <p>Not able to recruit diverse applicant pools.</p> <p>Weak recruitment program</p> | <p>HR reviews job vacancy notices prior to job posting.</p> <p>Job Description and Job Posting should be completed which thoroughly describes both the duties and the qualifications required of the individual.</p> <p>Review of the position description and FLSA designation should be done by higher authority before offer is made</p> <p>Within unit, have clear definition of authority to make commitment. Should have written procedures for all employment related processes that clearly outline authority levels, roles and responsibilities.</p> | <p>Develop organizational strategic plan or workforce plans.</p> <p>Division HR managers develop HR strategic plan that links to overall workforce objectives for the organization.</p> <p>Ensure managers and interviewers are provided resources regarding recruitment and selection laws and regulations.</p> <p>Review applicant flow information to ensure that HR staff is properly documenting applicant information in an accurate and timely manner and that records are current and available for appropriate review.</p> | <p>Review job openings and strategic plan to ensure organizational objectives are met.</p> <p>Ensure accurate EEO reports are prepared and submitted as required.</p> <p>Measure recruiting effectiveness by tracking and evaluating recruited employees and the total dollar costs of different recruiting methods.</p> <p>Conduct thorough job analysis on new positions to place them in correct title and level.</p> <p>Ensure there is a process for employees to request a review</p> |

| | | | | | |
|---|---|---|---|---|--|
| | | | <p>Observe required employment postings are posted in a location viewable by all employees</p> <p>Obtain recruitment action plans to determine whether they include budgets and time lines for addressing job vacancies and/or new positions.</p> <p>Determine whether the recruitment sources used are appropriate and adequate to produce a qualified and diverse applicant pool.</p> <p>Determine whether any applicant's tests or standardized scoring tools are used to ensure reliability and validity of the new hire.</p> <p>Review EEO/diversity plan regarding recruitment goals.</p> | <p>Develop process on how to place positions into appropriate job title and salary level.</p> | <p>of their position if they believe they are misclassified in an incorrect title or level.</p> <p>Make sure HR staff has appropriate expertise to perform job evaluation analysis.</p> |
| 3 | <p>Selection of Candidate -</p> <p>Ensure that candidate meets the qualifications and expectations for the position and represents themselves appropriately</p> | <p>Untrained managers ask illegal questions</p> <p>No standardized scoring tool to rank applicants on required job elements.</p> <p>Candidates selected do not fulfill requirements for position.</p> <p>Candidates misrepresent themselves.</p> <p>Documentation of the recruitment and selection process is incomplete or unavailable.</p> <p>Documenting inappropriate reasons for selection or non-selection.</p> <p>Final selection decision is not documented.</p> <p>Non-compliance with affirmative action plans.</p> <p>Nepotism.</p> <p>Discriminatory decisions in the hiring process.</p> | <p>Follow Hiring Guidelines (Recruitment and Selection policies).</p> <p>Unit must review PVL candidates if qualified consistent with announcement.</p> <p>Resumes and/or applications must be reviewed to ensure that they are consistent with the minimum requirements of the position.</p> <p>Review scoring tool or screening process to ensure it is appropriate and legal.</p> <p>Interviewers are trained in the types of questions and actions that are legal to ask in the hiring process.</p> <p>Ensure required applicants' test, if it is part of the selection process, is reliable and valid.</p> <p>Reference checks must be conducted on finalist(s)</p> <p>Background checks should be conducted that are consistent with the requirements of the position and to verify information reported in</p> | <p>Develop Recruitment and Selection policies and procedures.</p> <p>Establish benchmarking standards for the position.</p> <p>Search-and-screen committee or Interview panel is consisted of people knowledgeable about the position and the skills needed to perform in the vacant position.</p> <p>"No offer" (rejection) letters sent to all applicants.</p> <p>Ensure all employment documents are available, accurate and complete. (This includes applications, resumes, test results, interview questions, recruiting summary, reasons for hiring versus not hiring, and so forth.)</p> | <p>Review EEO/Diversity plan regarding recruitment goals and test EEO trends to determine whether progress is being made toward diversity goals.</p> <p>Review if EEO waiver requests for reasonableness.</p> <p>Hiring managers are trained in employment law.</p> <p>Hiring managers attend HR law seminar to gain updates in employment law and refresher training.</p> |

The University of Wisconsin – Extension
Internal Control Plan – March 2009

| | | | | | |
|---|---|--|---|--|---|
| | | | <p>application (e.g., education, prior employment history).</p> <p>Criminal background checks should be conducted on all applicants for positions of a sensitive nature (e.g., handle money.)</p> <p>Ensure compliance with Affirmative Action plan</p> <p>An approved management plan must be devised for potential nepotism situations.</p> <p>Ensure final selection decision is thoroughly documented. (This includes reasons for hiring versus not hiring.)</p> | | |
| 4 | <p>Job Offer -</p> <p>Ensure salary, conditions of employment, other commitments are appropriate</p> | <p>Erroneous or unauthorized salary, conditions of employment, or commitments.</p> <p>Inequality in salary</p> | <p>Make sure all background, criminal background and reference checks are conducted and results received before final offer was made.</p> <p>Review of position, FLSA designation, and salary to be done by higher authority before offer is made.</p> <p>Within unit, have clear definition of authority to make commitment.</p> <p>Obtain approval of offer by higher authority to approve terms of employment including salary before extending to candidate</p> <p>Offer letter should be completed.</p> <p>Document acceptance by employee</p> | <p>Determine if consistent criteria were used for making salary grade slotting.</p> <p>Review positions to ensure internal salary equity of positions across the organization.</p> | <p>Review salary actions to ensure they are nondiscriminatory.</p> |
| 5 | <p>Employment Eligibility –</p> <p>Verification-I9</p> <p>Ensure that proper documentation is examined and recorded</p> | <p>Violation of Immigration Laws</p> <p>Employee hired is not authorized to work in the US.</p> <p>Non-compliance with Federal Law, and fines.</p> | <p>I9 form completed in unit needs to be certified by a University employee who is knowledgeable and trained.</p> | <p>Units have identified and trained someone who can monitor that I9's in unit are being completed accurately, timely and completely.</p> | <p>Ensure all federal reports are prepared and submitted as required.</p> |
| 6 | <p>New Appointment -</p> <p>Ensure that new appointments contain accurate and appropriate pay rates, level of effort, effort distribution and</p> | <p>Incorrect salary, effort distribution or funding source</p> <p>Fraud</p> <p>Data entry errors</p> | <p>Hiring decision and offer letter should be retained</p> <p>Salary, short code, % effort, effective date should be approved by appropriate person who verifies that</p> | <p>Reconcile Gross Pay Register (GPR) to source documentation to ensure accurate & timely data entry.</p> | <p>Review salary actions to ensure they are nondiscriminatory.</p> |

The University of Wisconsin – Extension
Internal Control Plan – March 2009

| | | | |
|---|--|---|--|
| | funding sources | | it is consistent with offer letter. Verify data has been correctly entered into system |
| 7 | Change in Appointment – Ensure that changed appointments contain appropriate pay rate, level of effort, effort distribution and funding sources | Incorrect salary, effort distribution or funding source Fraud Data entry errors | Appointment Letter must be completed and signed by appropriate person Document & retain reason for change(s) Approval of salary/pay rate. Approval of level of effort to ensure that proper effort is reflected. Approval by higher authority documented. Perform reconciliation so errors are easily rectified in time to process any corrections in following month |

E-9 Control Matrix – Human Resources – Employment/Payroll Practices

| NO. | INTERNAL CONTROL | RISKS | KEY CONTROL POINTS | | |
|-----|--|--|---|---|--|
| | | | Operating Controls | Monitoring Controls | Oversight Controls |
| | Listed below are the sub-processes within the overall Employment process and what we are trying to control for within this sub-function. | This column lists risks inherent to the process which might cause inaccurate data or inaccurate activity. | | | |
| | Human Resources Development | | | | |
| 1 | New hired employee - Ensure that new employees are aware of all the human resource related policies and procedures | New employees lack understanding of the organization's culture and policies and procedures which are necessary skills and knowledge to perform their jobs. | <p>ALL new employees must attend new employee orientation within first 30 days of employment and receive Employee Handbook (policies and procedures) provided.</p> <p>New employee orientation to address the following issues:</p> <ul style="list-style-type: none"> • Insurance and benefits info • Grievance policy • Disciplinary action policy • Safety and security issues • Worker's compensation • Performance appraisal process • Sexual harassment issues • Employee leave policies • Americans with Disabilities Act • Equal employment opportunity related topics • Privacy, information security, code of ethics, and technology. <p>New employee orientation summary sheet must be signed off by all appropriate personnel for ALL new employees.</p> | HR is monitoring the training needs of the organization and making adjustments, and that the appropriate level of training for different positions is being offered. | No category of employees is excluded. |
| 2 | Newly hired supervisor/ Manager - Ensure new supervisors and managers trained on basic management principles and employment law. | <p>Untrained supervisors/managers to manage employees.</p> <p>Discrimination or harassment may occur due to improper frontline interaction with employees.</p> | <p>Supervisory training course to address the following issues:</p> <ul style="list-style-type: none"> • Basic management principals • Employment law • How to deal with employee issues • Employee performance management | <p>New managerial employees have attended management training within first 90 days after promotion/hire.</p> <p>Supervisors trained in performance management techniques, including how to recognize and address employee problems.</p> | Verify supervisory training is offered on a regular basis. |

The University of Wisconsin – Extension
Internal Control Plan – March 2009

| | | | | | |
|---|---|--|--|--|--|
| 3 | Training Program for Current Employees – | <p>Staff lacks ongoing technical training</p> <p>Lacked update skills and knowledge in today's "knowledge organization" environment.</p> <p>Training program cut has direct impact on performance and ultimately on the bottom's line.</p> | <p>Obtain any training catalogues or listings for available internal and external training.</p> <p>Employees who deliver training have received train-the-trainer instruction.</p> <p>Let employees aware of any tuition reimbursement policy where applicable.</p> | <p>HR reviews trends in performance problems and feeds this information into training program when appropriate.</p> | <p>Develop a process to assist in training plan development.</p> <p>Perform cost benefit analysis of different internal delivery methods (i.e., classroom, web-based training, and rotational job assignments) that are used for training.</p> <p>Review training information system to see if there is a single source that maintains information on external courses and seminars attended by employees.</p> |
| 4 | Ethics/Fraud Training | <p>Employees violate code of ethics.</p> <p>Employee lying on an employment application</p> <p>Employee stealing coworkers' possession.</p> <p>Employees not truthful about their work or work hours.</p> <p>Employees filed fraudulent workers' compensation.</p> | <p>Implementing appropriate policies</p> <p>Develop sound hiring practice (including thorough background checks), and providing ongoing fraud education for employees.</p> | <p>Provide training on fraud and or code of ethics.</p> <p>Establish an anonymous fraud reporting system and promote that system to employees.</p> | <p>Develop a process to ensure employees trained in these areas periodically.</p> |
| 5 | Benefits program – All employees are allowed to participate. The vesting period is the same for all employees in the same category. | <p>Employees are not aware of all the benefits available.</p> | <p>Ensure all employees receive copy of benefits program, including retirement, so they are aware of all the benefits available to them.</p> <p>Benefit program applies to all employees</p> | <p>Review benefits process with employees including enrollment, filing claims, challenging benefits determinations, and changing coverages.</p> | |
| | Employment practice | | | | |
| 6 | Performance appraisals | <p>Deficiency – does not adequately measure all aspects of the job.</p> <p>Contamination - items unrelated to job performance are evaluated.</p> <p>Evaluation errors - is not specific, objective, accurate and consistent.</p> <p>Past focus – used to rate past performance, rather than to improve future performance.</p> | <p>Develop effective employee performance appraisal programs to:</p> <ul style="list-style-type: none"> • Measure work performance as compared to job expectations. • Provide feedback and counseling. • Determine employees' and management's goals. • Identify employees' developmental needs. | <p>Ensure annual performance assessments are conducted, appropriate and approved performance standards have been established.</p> <p>Assess employee performance system to make sure that it adequately measure all aspects of the job, items evaluated are related to job performance, and is specific, objective, accurate</p> | <p>Ensure procedures are in place to maintain confidentiality of employee discussions when counseling employees on personal problems</p> <p>Make sure Employee Assistance program is available for employee.</p> <p>Make sure disciplinary actions are consistently applied for</p> |

The University of Wisconsin – Extension
Internal Control Plan – March 2009

| | | | | | |
|---|---|---|---|---|---|
| | | <p>Non-use – if people do not use it, we do not have a performance appraisal system.</p> <p>Disciplinary actions not properly documented.</p> <p>Include inappropriate language.</p> | <ul style="list-style-type: none"> • Provide documentation for future actions. • Allocate rewards and opportunities. <p>Performance appraisals are completed within time stated by policy; employee has signed form indicating the form was discussed with them and supervisor comments are job-specific and appropriate.</p> <p>HR is notified or consulted when a supervisor counsels an employee and puts him/her on a performance improvement plan so HR can follow-up to ensure appropriate support, action plan, employee acknowledgement, and final settlement can be documented.</p> <p>HR track all employee discipline actions and have documentation of performance or conduct issue, management steps taken, and final outcome of action.</p> | <p>and consistent. Performance appraisals should be focused on improving future performance, not to rate past performance.</p> <p>HR reviews performance sheets for inconsistencies across the organization.</p> <p>HR tracks and monitors appraisal due dates and notifies/reminds supervisors.</p> <p>HR reviews trends in performance problems and feeds this information into training program when appropriate.</p> | <p>similar problems across the organization.</p> |
| 7 | <p>Time Reporting –</p> <p>Ensure that timesheets or monthly attendance reports, if applicable, properly reflect hours worked and exception time taken.</p> <p>Procedures are followed consistently, including leaves taken under the Family Medical Leave Act or for outside activity.</p> | <p>Initial errors on timesheet or leave report completion</p> <p>Fraud</p> <p>Data entry errors.</p> <p>Timesheets not completed in timely manner; may result in incorrect payment or misuse of exception time</p> <p>Unclear policies on leaves reporting may lead to manipulation by employees.</p> | <p>Time sheet or leaves report should be completed/signed by employee themselves or supervisor under certain situations.</p> <p>Timesheets data entered locally by 3rd party - employee should not enter own timesheet or have special review of this time sheet.</p> <p>Timesheets entered on-line by employee should be approved by higher authority with knowledge of work schedule.</p> <p>Approval of timesheet or monthly attendance report by someone who can determine appropriateness of time reported.</p> <p>Approved timesheet should not be returned to employee but directly submitted to Payroll for processing.</p> | <p>Reconcile Gross Pay Register (GPR) to source documentation of appointment changes, exception time, and other payment related forms to ensure accurate & timely data entry; note any errors on report, attach correction documents and initial and date reconciliation</p> <p>Perform reconciliation so errors are easily rectified in time to process any corrections in following month</p> <p>Review to ensure that previous errors were corrected</p> | <p>Review Employment related Internal Control Reports for reasonableness and appropriateness</p> <p>Compare planned budgets to actual expenditures to ensure costs are consistent with expectations.</p> <p>Review vacation and sick time usage to identify potential issues regarding available balance.</p> |
| 8 | <p>Outside Activities Reporting -</p> <p>Procedures are followed consistently, including leaves</p> | <p>Initial errors on outside activities report completion</p> <p>Fraud</p> | <p>Outside consulting and outside teaching for personal gain are activities that could be perceived as material conflicts of interest. If an</p> | <p>If, during the year, significant changes in a staff member's reportable outside activities occur, the staff member shall</p> | <p>Promote Ethics training and provide clear guidance on outside activities reporting.</p> |

The University of Wisconsin – Extension
Internal Control Plan – March 2009

| | | | | | |
|----|--|--|---|--|---|
| | <p>taken for outside activity.</p> <p>Outside activities were approved by supervisors where applicable</p> | <p>Data entry errors.</p> <p>Violation of Code of Ethics such as utilization of work time for personal gain.</p> <p>Conflict of interest situation may exist when employee using his or position to gain or promote personal outside activities for pay.</p> | <p>employee is considering undertaking either of these activities for personal gain, the employee must notify his or her administrator before initiating the activity.</p> <p>Dean, director, or other appropriate administrator advises the staff member in writing within 15 days on the outside activity submitted.</p> <p>Provide training to employees to let them know that if outside consulting and owning a business done by employee as a private citizen thus must be done on the employee's own time and should not detract from his or her duties with the organization.</p> | <p>immediately inform, in writing, his or her dean, director, or other appropriate administrator.</p> <p>Requiring Outside Activities Reporting by April 30th.</p> | <p>Evaluate the reporting process to look for unusual trend and issues.</p> <p>Conduct analyses to determine reasonable reporting.</p> |
| 9 | <p>Retention/turnover costs -</p> <p>Ensure supervisors and managers consult with a HR representative before employees are suspended or fired.</p> | <p>Stress of worker shortage and "churn" which decreases productivity when turnover rate too high.</p> <p>Turnover costs may be higher than an employees' salary.</p> | <p>Conduct exit interview to determine the causes of turnover.</p> | <p>HR analyzes and takes actions on important issues brought out by the exit interviews or surveys.</p> | <p>HR computes employee turnover rate, reasons for turnover, and related replacement costs and review the results.</p> |
| | Payroll System | | | | |
| 10 | <p>Pay –</p> <p>Information regarding new hires, deductions, adjustments, terminations is communicated to payroll department.</p> | <p>Incorrect payment.</p> <p>Incorrect deductions.</p> <p>Fraud.</p> <p>Data entry errors.</p> | <p>Employees receive written policies and procedures (including unions') regarding the overall compensation administration program.</p> <p>Review salary structure with established salary grades and ranges within grades to ensure structure fully encompasses all employee salaries (i.e., employees are not paid below minimum or above maximum of salary grade range.)</p> | <p>Ensure compliance of Fair Labor Standards Act, Family Medical Leave Act</p> <p>Ensure payroll master file has accurate employee data.</p> | <p>Review procedure for analysis of position salaries compared to the market.</p> <p>Determine if there is any strategy in dealing with positions that significantly lead or lag the market.</p> |
| 11 | <p>Payroll System –</p> <p>Appropriate controls in place to safeguard payroll related information.</p> | <p>Payroll master file does not have accurate employee data.</p> <p>Payroll information was not communicated accurately (e.g., new hires, deductions, adjustments, terminations.)</p> <p>Weak controls in place to approve payroll file changes.</p> | <p>Access to payroll file data is restricted to authorized staff and the automated payroll data safeguarded with appropriate security controls.</p> <p>Reconcile payroll file and accounting records.</p> <p>Reconcile payroll file against tax reporting.</p> | <p>Determine whether technology up-to-date to provide accurate and timely payroll service.</p> <p>Verify that appropriate backup and recovery procedures exist for the payroll system.</p> <p>Make certain the employees have appropriate access the different levels of data.</p> | <p>Review a sample of management reports, tracing data to source system to verify accuracy of information.</p> <p>Ensure appropriate controls are in place to approve payroll file changes.</p> <p>Ensure access to payroll file data is restricted to authorized</p> |

The University of Wisconsin – Extension
Internal Control Plan – March 2009

| | | | | | |
|----|---|--|--|---|--|
| | | <p>Violation of Fair Labor Standards Act (FLSA) exempt or nonexempt status.</p> <p>Violation of FLSA overtime compensation requirements.</p> | <p>Ensure payroll deduction calculation is correct.</p> <p>Follow procedures regarding FLSA overtime compensation requirements.</p> | | <p>staff and automated payroll data is safeguarded with appropriate security controls.</p> <p>Review payroll report to detect any significant deviations.</p> <p>Review to determine whether supplemental payrolls are not used to regularly process regular payroll mistakes or oversights.</p> |
| 12 | <p>Promotions -</p> <p>Ensure that all promotion reviews and decision making follow both unit and University procedures.</p> | <p>Qualifications of position and individual could be inconsistent.</p> <p>Commitment of long term resources associated with achieving tenure.</p> <p>Non-compliance with affirmative action plans.</p> <p>Promotion and pay for performance increase are not supported by documented justification.</p> | <p>Ensure clear criteria for promotion and appropriately supported by documented justification.</p> <p>Clear understanding on who has the authority to make commitment.</p> <p>HR reviews salary actions to ensure they are nondiscriminatory.</p> | <p>Reconcile Gross Pay Register (GPR) to source documentation to ensure accurate & timely data entry; note any errors on report, attach correction documents and initial and date reconciliation</p> <p>Perform reconciliation so errors are easily rectified in time to process any corrections in following month</p> <p>Review to ensure that previous errors were corrected</p> | <p>Review salary actions to ensure they are nondiscriminatory.</p> |
| 13 | <p>Additional Pay –</p> <p>Additional pay is appropriate.</p> <p>Additional pay is for additional work, outside scope of original appointment</p> | <p>Errors on form completion</p> <p>Fraud</p> <p>Data entry errors</p> <p>Inconsistent with federal sponsor guidelines</p> <p>Inconsistent with FLSA overtime guidelines</p> <p>Work is within the scope of his/her appointment</p> <p>Work conflicts with primary job responsibilities</p> <p>Pay rate is excessive</p> | <p>Should utilize Additional Pay Submittal Form and/or approved batch processing; should be completed by appropriate person who has authority to hire employee for work outside normal employment, where appropriate</p> <p>Document and retain purpose for additional pay</p> <p>Approval by appropriate person including someone from unit in which individual has primary regular appointment. This person should be able to determine appropriateness of payment, including whether or not additional work is outside scope of regular appointment and if pay rate is appropriate</p> <p>Employee should not be processing their own paperwork</p> | <p>Reconcile Gross Pay Register (GPR) to source documentation of appointment changes, exception time, and other payment related forms to ensure accurate & timely data entry; note any errors on report, attach correction documents and initial and date reconciliation</p> <p>Perform reconciliation so errors are easily rectified in time to process any corrections in following month</p> <p>Review to ensure that previous errors were corrected</p> | <p>Review Employment related Internal Control Reports for reasonableness and appropriateness</p> <p>Compare planned budgets to actual expenditures to ensure costs are consistent with expectations</p> |

The University of Wisconsin – Extension
Internal Control Plan – March 2009

| | | | | | |
|--------------------------------|---|--|--|--|--|
| 14 | <p>Supplemental Pay –</p> <p>Ensure that payments are appropriate with regard to amount of payment and validity of payment</p> | <p>Errors on form completion</p> <p>Fraud,</p> <p>Erroneous or unauthorized expenditures</p> <p>Ineligible employees receiving payment</p> | <p>Utilize appropriate form consistent with unit and University policies and procedures.</p> <p>Approval by appropriate person</p> <p>Employee should not be processing their own paperwork</p> | <p>Reconcile GPR to source document or reconcile SOA to source document, depending on type of payment</p> | <p>Review Employment related Internal Control Reports for reasonableness and appropriateness</p> <p>Compare planned budgets to actual expenditures to ensure costs are consistent with expectations.</p> |
| 15 | <p>Exceptional Performance Pay -</p> <p>Ensure that employees that are eligible for exceptional performance pay are properly compensated</p> | <p>Fraud</p> <p>Erroneous or unauthorized expenditures</p> <p>Ineligible employees receiving payment</p> | <p>Documented calculation of Pay is separately performed by staff not receiving exceptional performance pay.</p> <p>Employee should not be processing their own paperwork</p> | <p>Adequacy of performance measures reviewed at pre-defined intervals</p> | <p>Review Employment related Internal Control Reports for reasonableness and appropriateness</p> <p>Compare planned budgets to actual expenditures to ensure costs are consistent with expectations.</p> |
| Other personnel matters | | | | | |
| 16 | <p>Personnel files -</p> <p>Ensure all employees' records/personnel files are kept in a secured location with controlled access and that they are kept in an environmentally safe location (i.e., fire/water/insect proof).</p> <p>Maintain records in accordance with all applicable laws.</p> | <p>Violation of records retention required by FMLA.</p> <p>Violation of OSHA records retention policy.</p> | <p>Review files to ensure:</p> <ul style="list-style-type: none"> • complete and appropriate information • Employee medical info, including family and medical leave and disability accommodation requests, is kept in files separate from general personnel file. • All Employment Eligibility Verification (I-9) forms and any other documentation identifying EEO data are kept separate from general personnel file. • Appropriate documentation and resolution are maintained in employee grievance files and are kept in a secure location <p>Certain FMLA records relating to employee's leave of absence are required to retain for three years.</p> <p>Make sure employee and supervisor are aware of the procedures to follow if an accident occurs.</p> <p>Review accident reports, showing documentation of personal injury and property damage.</p> <p>To comply with OSHA, make sure</p> | <p>HR has controls in place to ensure that they are aware of all employee complaints</p> <p>Analyzes the causes of complaints and grievances and makes recommendations for corrective and preventive measures to reduce the number of complaints and grievances filed.</p> | <p>Gather and maintain data on complaint for trends in the number and reasons for employee complaints or lawsuits against the organization.</p> <p>Determine if there are any employees utilizing the Americans with Disabilities Act (ADA) accommodation and ensure organization is in compliance with the law.</p> |

The University of Wisconsin – Extension
Internal Control Plan – March 2009

| | | | | | |
|----|--|--|---|--|--|
| | | | <p>that all records of job-related injuries and illnesses be kept for five years.</p> <p>Records related to medical exams along with toxic substances and blood-borne pathogen exposure must be retained for thirty years after termination of employment.</p> | | |
| 17 | <p>Risk/safety management –</p> <p>Determine whether workplace health, safety, and security plans are effective.</p> <p>Ensure compliance with all applicable regulations.</p> | <p>Employees not aware of emergency management policies and procedures.</p> <p>COOP, DRP, and OEP have not been communicated to employees.</p> <p>Discrimination risks.</p> <p>Workers compensation risks.</p> <p>No reserve to pay or defend employment claims.</p> | <p>Make sure employees are trained on emergency procedures.</p> <p>Conduct self-assessments of HR policies and procedures to identify potential risk.</p> <p>Identify potential risk areas.</p> <p>Follow-up with complaints.</p> | <p>Review worker’s compensation data reports and safety incident reports.</p> <p>Track historical employment losses (legal expenses, settlement payments, investigations costs) to measure the success of the employment practices, particularly on safety issues.</p> | <p>Compare trend data to industry reports for safety issues.</p> <p>Establish privacy policies and make sure appropriate controls to protect employees (e.g., identify theft, personal data protection, HIPAA compliance.)</p> <p>Develop a method of quantifying the dollars of exposure the organization may have from discrimination risks or safety risks.</p> |
| 18 | <p>Termination of Employee –</p> <p>Ensure that employees are properly terminated</p> | <p>Employee continues to be paid.</p> <p>Employee continues to have access to systems/databases/building.</p> <p>Rehiring of inappropriate employee</p> | <p>Termination paperwork and employee termination checklist should be completed by appropriate person (typically by supervisor during the exit interview) who can verify that each step of termination has been successfully completed.</p> <p>Sign-off by appropriate person(s) to ensure all terminations are processed such as computer access is terminated, key(s) to the building has been returned, etc.</p> | <p>Ensure that COBRA notifications sent to terminated employees within two weeks after notification of termination.</p> <p>Review GPR within 30 days to ensure employee has been removed</p> | <p>Review employee turnover rate report, reasons for turnover and related replacement costs.</p> <p>Selects a sample of terminated employees and obtain evidence that appropriate procedures were followed.</p> |

E-10 Control Matrix – Information Technology – General Controls

| NO. | INTERNAL CONTROL | RISKS | KEY CONTROL POINTS | | |
|-----|---|---|--|---|---|
| | | | Operating Controls | Monitoring Controls | Oversight Controls |
| | Listed below are the sub-processes within the overall Information Technology (IT) process and what we are trying to control for within this sub-function. | This column lists risks inherent to the process which might cause inaccurate data or inaccurate activity. | | | |
| | Security Policy | | | | |
| 1 | Overall security policies | Isolated data centers, Developers requesting non-standard business/security practices. | Ensure applied controls meet the approved security specification for the software and hardware and implement the organizations' security policy or meet industry standards. Use of firewalls/access control lists. | Tripwire, intrusion deception, network syslogs | Ensure standards and processes are in place to secure access based on business need |
| 2 | User access security – | Unauthorized users access to organization's servers and browse sensitive files with the guest ID. Access to unauthorized data. Not aware of unauthorized changes or deletions. Individual not clear about individual responsibilities. | Restrict access. Access approved only to applications/data files authorized by supervisor in accordance to established authorization procedures. Usage and changing of passwords. Disable the guest ID. | Perform periodic system security review and testing to ensure adequate security is provided for all the servers. Verification of information through observation of actual practices and reviewing printed output where available. | Develop access policy and procedures. User awareness – education and training. |
| 3 | Vendor access security – | Unauthorized access to data files. | Restrict access, access approved in accordance with established authorization procedures. | Firewall ACL, system permission ACL, system logs. | No generic accounts, one per vendor. |
| 4 | Data security – Ensure confidentiality, integrity, authentication and non-repudiation. | Users not clear about data security policy. Data leaks. Sensitive data exposed. Data manipulated. Errors not detected. Programmers change live data inappropriately. | All data changes made by programmers be logged and reviewed by appropriate custodian of data. Review operation log. | Verification of information by reviewing printed output where available. All changes made to data must be logged and reviewed by supervisory personnel. Verify the integrity of a sequence of data bits. | Set policy about secured IM platforms. Disaster recovery planning. |

The University of Wisconsin – Extension
Internal Control Plan – March 2009

| | | | | | |
|--------------------------|---|---|--|--|---|
| 5 | Applications maintenance | Unauthorized personnel have access to the source code library. Programmers have access to live data files. | All work by programmers should be logged and reviewed by supervisors. Implementing version control. | Access to code is logged. | Logs are kept for one year. |
| 6 | Technical security | Adequate controls on devices. No default vendor passwords. | Source code/document version control procedures are in place to protect the integrity of program code | System logs of access to servers. | Develop policies and procedures to help users perform more efficiently and report problem |
| 7 | Hardware/software configuration, installation, testing, management standards, policies and procedures | Software not kept up to date. Need to update servers. | Ensure applied controls meet the approved security specification for the software and hardware and implement the organizations' security policy or meet industry standards. | Systems are monitored for vendor updates. (WSUS, RHN) | Keep track of systems, remove unneeded devices. |
| Physical Security | | | | | |
| 8 | Perimeter security | No control over the use of computer resources. | Security provided by electronic card readers An audit trail of who has accessed the facility Video surveillance is also configured within the Data Center Remote KVM console and RILO controls for servers housed within the Data Center allows staff to have full control of equipment without requiring physical access | Logs are kept of who accessed the data center via card access. | Cameras are placed in the data Center. UW Police have access to the data. |
| 9 | Operations room security | Unauthorized personnel have access to the operations room. | Only authorized personnel admitted to the computer operations room. Computer room(s) is locked. | Verification by observation of actual practices. | Cameras are placed in the Data Center. |
| 10 | Terminal physical access | Unauthorized personnel have access to the terminal. | All terminals used for administrative computing are located in areas under supervision during normal working hours. The areas are locked after hours. | Logs are kept on access to administrative areas. | |

The University of Wisconsin – Extension
Internal Control Plan – March 2009

| | | | | | |
|----|---|--|--|---|--|
| 11 | System back up | Operations interrupted. Delay recovery due to lost of data. | Data is backed up on a daily, weekly and monthly basis. Two generations of backup, with one stored off site. | Backup logs are reviewed by staff. | Files are periodically tested and restored. |
| 12 | Hardware/software configuration, installation, testing, management standards, policies and procedures | Wrong patch can cause wide scale outage. | Ensure applied controls meet the approved security specification for the software and hardware and implement the organizations' security policy or meet industry standards. | Update servers and track patches applied. | Logs are reviewed by staff. |
| | Change Management | | | | |
| 13 | Change Management - Procedures are in place to ensure changes meet business requirements and are authorized. | Unauthorized changes to program or data. | Ensure standardized methods, processes and procedures are used for all changes. Facilitate efficient and prompt handling of all changes. Maintain the proper balance between the need for change and the potential detrimental impact of changes. Segregation of responsibilities between program changes and program storage. Testing conversion, implementation and documentation. | Externally imposed requirements e.g., legislative changes | Implementing an organizational structure with well-defined roles for the responsibility of information, business processes, applications, infrastructure, etc. |
| 14 | Software development life cycle standards have been established to ensure IT projects are effectively managed | Invalid code can lead to system compromise. | Ensure applied controls meet the approved security specification for the software and hardware and implement the organizations' security policy or meet industry standards. Restricting access to system documentation, software and operations to authorized personnel only. New programs development authorized in accordance with system design standards and documentation standards. | | |

The University of Wisconsin – Extension
Internal Control Plan – March 2009

| | | | | | |
|----|---|--|--|--|--|
| 15 | Incident management | Improper investigation by staff can lead to compromised data. | Incidents are investigated by staff. | Events are correlated with external logs. | Develop policies and procedures designed to address operational processing errors |
| | Threat | | | | |
| 16 | Disaster recovery/backup and recovery procedure to enable continued processing despite adverse conditions | Likelihood of threat exploitation Magnitude of impact Inadequacy of planned or current controls. | Daily Backup tapes generated. One backup tape stored off site. Offsite storage of data and computer programs. Alternative processing facilities. | Protection of backup copies. | Develop adequate backup and recovery procedures. |
| 17 | System – | System vulnerabilities were not identified. Unauthorized system access (access to classified, proprietary, and/or technology-related information) System intrusion, break-ins. | Performance of system security testing | Development of a security requirements checklist. | Organization's security, policies, planned security procedures, and system requirement definitions, and the vendors' or developers' security product analyses are incorporated into the system design. Review IT system's audit reports, system anomaly reports, security review reports, and system test and evaluation reports. |
| 18 | Hacker, cracker | Hacking Social engineering System intrusion, break-ins Unauthorized system access | Watch out for the following motivation: challenge, ego, rebellion Automated vulnerability scanning tool test | System logs are reviewed for inappropriate activities. | Development and execution of a test plan (e.g., test script, test procedures, and expected test results) to test the effectiveness of the security controls of the system. |
| 19 | Computer criminal | Fraudulent act (e.g., replay, impersonation, interception) Computer crime (e.g., cyber stalking) System intrusion Spoofing Information bribery | Watch out for the following motivation: destruction of information, illegal information disclosure, monetary gain, unauthorized data alteration. Automated vulnerability scanning tool test | System logs are reviewed for inappropriate activities. | Policies on inappropriate use are enforced. |
| 20 | Terrorist | Bomb/Terrorism Information warfare System attack (e.g., distributed denial of service) | Watch out for the following motivation: blackmail, destruction, exploitation, revenge. Perform penetration testing | System logs are reviewed for inappropriate activities. | Policies on inappropriate use are enforced. |

| | | | | | |
|----|----------------------|--|---|---|---|
| | | System penetration System tampering | | | |
| 21 | Industrial espionage | Economic exploitation Unauthorized system access (access to classified, proprietary, and/or technology-related information) Intrusion on personal privacy Information theft Social engineering System penetration | Watch out for the following motivation: competitive advantage, economic espionage Perform penetration testing | System logs are reviewed for inappropriate activities | Policies on inappropriate use are enforced. |
| 22 | Insiders | Assault on an employee Blackmail Browsing of proprietary information Computer abuse Fraud and theft Information bribery Input of falsified, corrupted data interception Malicious code (e.g., virus, logic bomb) Unintentional errors and omissions (e.g., data entry error, programming error) Revenge, curiosity, ego or monetary gain. Sale of personal information System bugs, intrusion, sabotage Unauthorized system access | Watch out for poorly trained, disgruntled, malicious, negligent, dishonest, or terminated employee. Automated vulnerability scanning tool test | System logs are reviewed for inappropriate activities | Policies on inappropriate use are enforced. |

The University of Wisconsin – Extension
Internal Control Plan – March 2009

| | | | | | |
|----|--|--|---|---|--|
| 23 | Environmental conditions | Data center may be destroyed by: Fire/smoke Flood/water Temperature Humidity Door position | Installation of water sprinklers to put out a fire automatically to suppress fire. Online monitoring system which can notify staff via email, page, and phone in cases of emergency. 80kW of electrical power available for powering a computing equipment that is conditioned and protected via the UPS in an N+1 battery configuration An onsite diesel generator with capacity to supply an electrical current of 150 amps at 480 volts in event of loss of main power Computer systems located in the Data Center will be set up with a minimum runtime to convert to backup electrical power Cooling is provided via 6 chilled water In-row air conditioning units The air conditioners capture heat directly from the hot aisle in the rack configuration and distribute cool air | Data Center monitors environmental conditions. Alerts are sent to staff when necessary. | Logs are kept and reviewed by appropriate staff. |
| | Others | | | | |
| 24 | Hardware disposal/transfer to other entities | Records, containing personally identifiable information, not properly erased. | Follow established process to ensure any hardware that contains sensitive information is properly erased before disposal. | Ensure established process has been followed. | Develop standardized process to properly erase records still reside in the hardware. |
| 25 | Network | Records maintained on a network where access is not properly restricted. | Firewalls provide access to resources. | Firewall logs are kept and reviewed. | Log process is monitored for accuracy. |
| 26 | Files | Turnover in departments has led to the loss of electronic files when employees leave and either they or their replacement purges old files without realizing the need for retention. | Follow procedures to archiving and retaining documents electronically. | File level monitoring is performed on select systems. | Develop a plan for archiving and retaining documents electronically to safely meet long-term retention requirements. |

The University of Wisconsin – Extension
Internal Control Plan – March 2009

| | | | | | |
|----|-----------|---|---|---|---|
| | | Unauthorized individuals obtaining personal information that could be used in inappropriate disclosure or identity theft. | | | |
| 27 | Archiving | <p>Departments have migrated into an electronic filing/archiving mode without any forethought or planning for file protection, sharing, archiving and backup.</p> <p>Unauthorized individuals obtaining personal information that could be used in inappropriate disclosure or identity theft.</p> <p>Lack of a plan for archiving and sharing documents has resulted in documents being irretrievable because the originator password protected them and subsequently left or doesn't remember the password used several years ago.</p> <p>Changes in software can make documents from earlier products difficult if not impossible to retrieve.</p> | Select systems can be archived for later access. No systematic approach has been developed. | A log of archives is created when a system has been archived. | Develop a plan to perform archiving on important files. |

E-11 Control Matrix – Information Technology – Application Controls

| NO. | INTERNAL CONTROL | RISKS | KEY CONTROL POINTS | | |
|-----|---|---|--|---|---|
| | | | Operating Controls | Monitoring Controls | Oversight Controls |
| | Listed below are the sub-processes within the overall Information Technology (IT) Application process and what we are trying to control for within this sub-function. | This column lists risks inherent to the process which might cause inaccurate data or inaccurate activity. | | | |
| 1 | <p>Input controls –</p> <p>Ensure all transactions are initially recorded and processed only once.</p> <p>Ensure data integrity fed from upstream sources into the application system</p> | <p>Transactions are not recorded correctly.</p> <p>Transactions processed more than once.</p> <p>Transactions recorded on inappropriate computer data files.</p> <p>Transactions processed are not authorized or checked.</p> | <p>Record counts, control or batch totals and hash totals.</p> <p>Validity check are conducted to ensure only valid data is input or processed.</p> <p>Reasonableness tests, limit test, field checks.</p> | Clerical/divisions/offices review of input transactions. | Inspect validation procedure. |
| 2 | <p>Processing Control –</p> <p>Ensure all transactions input are accepted and processed completely through all stages of processing.</p> | Transactions are not processed correctly. | <p>Control total.</p> <p>Error log.</p> <p>File labels.</p> <p>Overflow tests.</p> <p>Cross footing tests.</p> <p>Control access to programs and data files by using passwords.</p> | <p>Supervision of operator activities.</p> <p>Control access to programs and data files by review of computer logs.</p> | Review exception reports. |
| 3 | <p>Output Control –</p> <p>Ensure all records were processed from initiation to completion correctly.</p> | <p>Transactions are not recorded correctly.</p> <p>Transactions processed more than once.</p> <p>Transactions recorded on inappropriate computer data files.</p> <p>Transactions processed are not authorized or checked.</p> | <p>Review of output by control groups and users in determining the overall reasonableness of processing controls.</p> <p>Reconcile output control totals with input and processing control totals (compared with source documents.)</p> <p>Completeness checks to ensure all records were processed.</p> | Review summary of transactions produced after each application is finished for the day. | Review reconciliation of totals by user department. |

The University of Wisconsin – Extension
 Internal Control Plan – March 2009

| | | | | | |
|---|---|--|---|--|--------------------------------|
| 4 | <p>Identification –</p> <p>Ensure all users are uniquely and irrefutable identified</p> <p>Ensure all application problems are recorded and managed in a timely manner.</p> | <p>Unauthorized access or processes.</p> <p>Errors not caught or correct in a timely manner.</p> | <p>Ensure computer operators are programmers.</p> <p>Users of each application correct their own errors in source documents.</p> <p>All item identification numbers are validated against master files.</p> | <p>Inspect error log for errors corrected.</p> | |
| 5 | <p>Authentication –</p> <p>Provide an authentication mechanism in the application system.</p> <p>Ensure all changes on production environment are implemented with preserved data integrity</p> | <p>Unauthorized access or processes.</p> <p>Errors not caught or correct in a timely manner.</p> | <p>The data files are backup at the end of each day.</p> | <p>Ensure backup procedures are followed.</p> | <p>Review backup procedure</p> |

E-12 Control Matrix – Payment Card Data Security Controls (Processed/Stored by UWEX)

| NO. | INTERNAL CONTROL | RISKS | KEY CONTROL POINTS | | |
|-----|---|---|--|---|---|
| | | | Operating Controls | Monitoring Controls | Oversight Controls |
| | Listed below are the sub-processes within the overall Information Technology (IT) Application process and what we are trying to control for within this sub-function. | This column lists risks inherent to the process which might cause inaccurate data or inaccurate activity. | | | |
| | Information Security Policy | | | | |
| 1 | Security policy established, published, maintained, and disseminated. | Employees not aware of security policy. Sensitive data not secured in accordance with the policy. | Follow established security policy and procedures. Failure to adhere to security policy and established procedures may result in disciplinary action. | Develop security policy to include a review at least once a year and updates when the environment changes. Develop usage policies for critical employee-facing technologies (e.g., remote-access technologies, wireless technologies, removable electronic media, laptops, personal data/digital assistants, e-mail, and Internal usage) to define proper use of these technologies for all employees and contractors. | Ensure security policy and procedures clearly define information security responsibilities for all employees and contractors. Make sure employees aware of the importance of cardholder data security. |
| | Secured network | | | | |
| 2 | Firewall configuration – Formal process Standardize configuration. | Cardholder data may be compromised by unauthorized access - outside attacker, inside attacker, data entry people jotting down numbers | Follow established firewall configuration standards for: <ul style="list-style-type: none"> • Approving and testing all external network connections and changes. • Create network diagram with all connections to cardholder data, including any wireless networks. • Firewall at each Internet connection and between any demilitarized zone (DMZ) and the internal network zone. • Hypertext transfer protocol (HTTP), and secure sockets layer (SSL), secure shell (SSH), and virtual private network (VPN) are allowed protocol • Include routers | Develop firewall configuration standards to include: <ul style="list-style-type: none"> • Formal process for approving and testing all external network connections and changes to the firewall configuration. • Current network diagram documents all connections to cardholder data and that the diagram is consistent with the firewall configuration, including internet connection and the DMZ. • Description of groups, roles, and responsibilities for logical management of network components • List of services/ports necessary for business | Management approval of all changes to external connections and firewall configuration. Ensure the diagram is kept current. Examine documentation and settings for each service in use to obtain evidence that the service is necessary and secured. Quarterly review of firewall and router rule sets. |

| | | | | | |
|---|--|--|--|--|--|
| | | | | <ul style="list-style-type: none"> • Require justification and documentation for any available protocols besides HTTP and SSL, SSH, and VPN as well as any risky protocols allowed (e.g., FTP), which includes reason for use of protocol, and security features implemented. | |
| 3 | <p>Firewall configuration -</p> <p>Restrict connections with untrusted networks and any system in the cardholder data environment.</p> | Unauthorized access to sensitive data. | <p>Build a firewall configuration that denies all traffic from “untrusted” network and hosts, except for protocols necessary for the cardholder data environment.</p> <p>Build a firewall configuration to include:</p> <ul style="list-style-type: none"> • Restricting inbound Internet traffic to internet protocol (IP) addresses within the (ingress filters) • Not allowing internal addresses to pass from the Internet into the DMZ • Only “established” connections are allowed into the network • Placing the database in an internal network zone, segregated from the DMZ • Restricting inbound and outbound traffic to that which is necessary for the cardholder data environment • Securing and synchronizing router configuration files. • Denying all other inbound and outbound traffic not specifically allowed. • Installing perimeter firewalls between any wireless networks and the cardholder data environment, and configuring these firewalls to deny any traffic from the wireless environment or from controlling any traffic • Installing personal firewall software on any laptops which are used to access the organization’s network. | <ul style="list-style-type: none"> • Examine firewall and router configurations to verify that inbound and outbound traffic is limited to only protocols that are necessary for the cardholder data environment and connections are restricted between publicly accessible servers and components storing cardholder data. • Examine firewall/router configurations to include the choke router at the Internet, the DMZ router and firewall, the DMZ cardholder segment, the perimeter router, and the internal cardholder network segment. | <p>Management approval of all changes to external connections and firewall configuration.</p> <p>Ensure the diagram is kept current.</p> <p>Examine documentation and settings for each service in use to obtain evidence that the service is necessary and secured.</p> <p>Quarterly review of firewall and router rule sets.</p> |

The University of Wisconsin – Extension
Internal Control Plan – March 2009

| | | | | | |
|----------------------------|--|---|---|---|--|
| 4 | <p>Firewall configuration -</p> <p>Prohibit direct public access between the Internet and any system component in the cardholder data environment.</p> | <p>Public access to databases, logs, trace files could be problematic</p> | <p>Implement a DMZ to filter and screen all traffic and to prohibit direct routes for inbound and outbound internal traffic.</p> <p>Restrict outbound traffic from payment card applications to IP addresses within the DMZ.</p> | <p>Examine firewall/router configurations and verify there is no direct route inbound or outbound for Internet traffic.</p> <p>Examine firewall/router configurations and verify that internal outbound traffic from cardholder applications can only access IP addresses within the DMZ.</p> | <p>Management approval of all changes to external connections and firewall configuration.</p> <p>Ensure the diagram is kept current.</p> <p>Examine documentation and settings for each service in use to obtain evidence that the service is necessary and secured.</p> <p>Quarterly review of firewall and router rule sets.</p> |
| 5 | <p>Firewall configuration –</p> <p>Implement IP masquerading to prevent internal addresses from being translated and revealed on the Internet.</p> | <p>Unauthorized access to sensitive data.</p> | <p>Use technologies that implement RFC 1918 address space, such as port address translation (PAT) or network address translation (NAT).</p> | <p>Restrict broadcast of IP addresses from the internal network to the Internet (IP masquerading).</p> | <p>Examine documentation and settings for each service in use to obtain evidence that the service is necessary and secured.</p> <p>Quarterly review of firewall and router rule sets.</p> |
| Security parameters | | | | | |
| 6 | <p>Vendor-supplied defaults –</p> <p>Changed before installing a system on the network.</p> | <p>Unauthorized access to sensitive data.</p> | <p>Vendor-supplied defaults always changed before installing a system on the network:</p> <ul style="list-style-type: none"> - passwords, - simple network management protocol - community strings - elimination of unnecessary accounts <p>Non-console administrative access encrypted (use of SSH, VPN or SSL/TLS)</p> <p>Change wireless vendor defaults. Disable service set identifier (SSID) broadcasts. Enable WiFi protected access technology for encryption and authentication when WIPA capable.</p> | <p>Ensure system components, critical servers, and wireless access points can not be accessed using default vendor-supplied account and passwords.</p> <p>Ensure vendor default settings for wireless environments have been changed.</p> | <p>Forbids the use of default passwords.</p> |

The University of Wisconsin – Extension
Internal Control Plan – March 2009

| | | | | | |
|---|--|---|---|--|---|
| 7 | <p>Cardholder data –</p> <p>Ensure system adhere to requirements regarding storage of sensitive authentication data after authorization (even if encrypted).</p> | <p>Data breach. Personal data such as Social Security Numbers and birthdays stolen.</p> <p>Criminal with the stolen data can complete at least one or two purchases before discovery</p> <p>An "unauthorized individual" infiltrated the computer network of a third-party payment processor and may have stolen up to 40 million credit card numbers</p> | <p>Store only the following data elements:</p> <ul style="list-style-type: none"> • The cardholder's name • Primary account number • Expiration date • Service code. <p>Primary account number is masked when displayed.</p> <p>Encrypt the data</p> <p>Call data emergency personnel if data breach is discovered.</p> <p>Any information or hard copies of credit cards or bank accounts available must be kept confidential and protected from misuse. Current records/hard copies must be locked in secured places.</p> <p>Only authorized personnel should have access to the locked/secured places.</p> <p>Follow Records Retention Schedule.</p> | <p>Ensure card verification code or value or PIN verification value data elements or the encrypted PIN block are not stored.</p> <p>Full contents of any track from the magnetic stripe are not stored.</p> <p>Ensure security policy and procedures are adhered to.</p> <p>Maintain separation of duties and accountability.</p> | <p>Ensure employees are trained on security issues.</p> |
| 8 | <p>Encrypt transmission of cardholder data across open, public networks</p> | <p>Unauthorized access to sensitive data.</p> | <p>Use strong cryptography and security protocols, such as SSL/TLS or IPSEC, is used to safeguard sensitive cardholder data during transmission over open, public networks (e.g., Internet, wireless technologies, etc.)</p> <p>Use unique and independent network.</p> | <p>Develop policies and procedures to preclude the sending of unencrypted Primary Account Numbers by end-user messaging technologies (e.g., e-mail, instant messaging, and chat).</p> <p>Ensure credit card and bank information are not stored on any personal or work computer.</p> <p>No email of sensitive information.</p> <p>No unauthorized access to secured places where sensitive information is stored.</p> | <p>Ensure employees are trained on security issues.</p> |
| 9 | <p>Vulnerability Management</p> <p>Use and regularly update anti-virus software or programs</p> | <p>An unauthorized entity put a specific code into Card Systems' network," enabling the person or group to gain access to the data</p> | <p>Anti-virus software deployed on all systems, particularly personal computers and servers commonly affected by malicious software.</p> | <p>Mandating the proper use of firewalls, message encryption, computer access controls and antivirus software.</p> | <p>Requires frequent security audits and network monitoring.</p> <p>Require internal and external network vulnerability scans run</p> |

The University of Wisconsin – Extension
Internal Control Plan – March 2009

| | | | | | |
|----|--|--|--|---|--|
| | Develop and maintain secure systems and applications. | | <p>Scan payment software for vulnerabilities.</p> <p>Anti-virus mechanisms actively running and capable of generating audit logs.</p> <p>additional firewalls and access controls</p> <p>System components and software have the latest vendor-supplied security patches installed.</p> <p>Critical security patches installed within one month of release.</p> | <p>Review audit log for potential problems.</p> <p>Ensure anti-virus programs capable of detecting removing and protecting against all known types of malicious software.</p> | <p>at least quarterly and after any significant change in the network (such as new system component installations, changes in network topology, firewall rule modifications, product upgrades.)</p> |
| 10 | <p>Access control measures –</p> <p>Restrict access to cardholder data by business need-to-know.</p> | Unauthorized access to sensitive data. | <p>Access to system components and cardholder data limited to only those individuals whose jobs require such access.</p> <p>Assign a unique ID to each person with computer access.</p> <p>Accounts used by vendors for remote maintenance enabled only during the time period needed.</p> | <p>Approve access request.</p> <p>Test the presence of wireless access points by using a wireless analyzer at least quarterly or by deploying a wireless IDS/IPS to identify all wireless devices in use to ensure proper control is in place is.</p> | <p>Ensure employees are trained on security issues and importance of cardholder data security.</p> |
| 11 | <p>Access control measures –</p> <p>Restrict physical access to cardholder data.</p> | Unauthorized access to sensitive data. | <p>All paper and electronic media that contain cardholder data physically secure.</p> <p>Strict control over the internal or external distribution of any kind of media that contains cardholder data.</p> <p>Identify cardholder data as confidential.</p> <p>Tracked media sent by secured courier or other deliver method that can be accurately tracked,</p> <p>Hardcopy materials shredded, incinerated, or pulped so that cardholder data cannot be reconstructed.</p> | <p>Develop processes and procedures to ensure management approval is obtained prior to moving any and all media containing cardholder data from a secured area (especially when media is distributed to individuals.)</p> | <p>Observe strict control be maintained over the storage and accessibility of media that contains cardholder data and destruction of data when it is no longer needed for business or legal reasons.</p> |

E-13 Control Matrix – Payment Card Data Security Controls (Processed/Stored by Vendor)

| NO. | INTERNAL CONTROL | RISKS | KEY CONTROL POINTS | | | |
|-----|---|---|---|---|---|--------------------|
| | Listed below are the sub-processes within the overall Information Technology (IT) Application process and what we are trying to control for within this sub-function. | This column lists risks inherent to the process which might cause inaccurate data or inaccurate activity. | Operating Controls | | Monitoring Controls | Oversight Controls |
| | Information Security Policy | | | | | |
| 1 | Security policy established, published, maintained, and disseminated. | Employees not aware of security policy. Sensitive data not secured in accordance with the policy. | Follow established security policy and procedures. Failure to adhere to security policy and established procedures may result in disciplinary action. Hypertext transfer protocol (HTTP), and secure sockets layer (SSL), secure shell (SSH), and virtual private network (VPN) are allowed protocol. | Develop security policy to include a review at least once a year and updates when the environment changes. Develop usage policies for critical employee-facing technologies (e.g., remote-access technologies, wireless technologies, removable electronic media, laptops, personal data/digital assistants, e-mail, and Internal usage) to define proper use of these technologies for all employees and contractors. | Ensure security policy and procedures clearly define information security responsibilities for all employees and contractors. Make sure employees aware of the importance of cardholder data security. | |
| | Security parameters | | | | | |
| 2 | Cardholder data – No electronic storage of credit cards and bank account information because e-payments are processed by outside vendor. | Data breach. Personal data such as Social Security Numbers and birthdays stolen. | Call data emergency personnel if data breach is discovered. Any information or hard copies of credit cards or bank accounts available must be kept confidential and protected from misuse. Current records/hard copies must be locked in secured places. Only authorized personnel should have access to the locked/secured places. Follow Records Retention Schedule. | Ensure security policy and procedures are adhered to. Maintain separation of duties and accountability. | Ensure employees are trained on security issues. | |

The University of Wisconsin – Extension
Internal Control Plan – March 2009

| | | | | | |
|---|---|---|---|--|--|
| 3 | <p>Transmission of cardholder data across open, public networks</p> <p>No electronic storage of credit cards and bank account information because e-payments are processed by outside vendor.</p> | <p>Data breach. Personal data such as Social Security Numbers and birthdays stolen.</p> <p>Unauthorized access to sensitive data.</p> | <p>If applicable, being a point-of-entry, sensitive data should only be entered in designated secured computers, which should not have other software or programs, and by authorized users only.</p> <p>Use unique and independent network.</p> <p>Use strong cryptography and security protocols, such as SSLTLS or IPSEC, is used to safeguard sensitive cardholder data during transmission over open, public networks (e.g., Internet, wireless technologies, etc.)</p> <p>Never email sensitive information.</p> <p>If receive an email with sensitive data, process as needed, delete the email and empty the deleted items folder.</p> | <p>Ensure credit card and bank information are not stored on any computer.</p> <p>No email of sensitive information.</p> <p>No unauthorized access to secured places where sensitive information is stored.</p> | <p>Ensure employees are trained on security issues.</p> |
| 4 | <p>Vulnerability Management</p> <p>Use and regularly update anti-virus software or programs</p> <p>Develop and maintain secure systems and applications.</p> | <p>Data breach. Personal data such as Social Security Numbers and birthdays stolen.</p> <p>Unauthorized access to sensitive data.</p> | <p>Anti-virus software deployed on all systems, particularly personal computers and servers commonly affected by malicious software.</p> <p>Anti-virus mechanisms actively running and capable of generating audit logs.</p> <p>Additional firewalls and access controls</p> <p>System components and software have the latest vendor-supplied security patches installed.</p> <p>Critical security patches installed within one month of release.</p> | <p>Mandating the proper use of firewalls, message encryption, computer access controls and antivirus software.</p> <p>Review audit log for potential problems.</p> <p>Ensure anti-virus programs capable of detecting removing and protecting against all known types of malicious software.</p> | <p>Requires frequent security audits and network monitoring.</p> <p>Require internal and external network vulnerability scans run at least quarterly and after any significant change in the network (such as new system component installations, changes in network topology, firewall rule modifications, product upgrades.)</p> |
| 5 | <p>Access control measures –</p> <p>Restrict access to cardholder data by business need-to-know.</p> | <p>Unauthorized access to sensitive data.</p> | <p>Access to system components and cardholder data limited to only those individuals whose jobs require such access.</p> <p>Assign a unique ID to each person with computer access.</p> | <p>Approve access request.</p> | <p>Ensure employees are trained on security issues and importance of cardholder data security.</p> |

The University of Wisconsin – Extension
Internal Control Plan – March 2009

| | | | | | |
|---|---|---|--|---|--|
| 6 | <p>Access control measures – Restrict physical access to cardholder data.</p> | <p>Unauthorized access to sensitive data.</p> | <p>All paper and electronic media that contain cardholder data physically secure.</p> <p>Strict control over the internal or external distribution of any kind of media that contains cardholder data.</p> <p>Identify cardholder data as confidential.</p> <p>Tracked media sent by secured courier or other deliver method that can be accurately tracked,</p> <p>Follow Records Retention Schedule.</p> <p>Hardcopy materials shredded, incinerated, or pulped so that cardholder data cannot be reconstructed.</p> | <p>Develop processes and procedures to ensure management approval is obtained prior to moving any and all media containing cardholder data from a secured area (especially when media is distributed to individuals.)</p> | <p>Observe strict control be maintained over the storage and accessibility of media that contains cardholder data and destruction of data when it is no longer needed for business or legal reasons.</p> |
|---|---|---|--|---|--|