

# STANDARDS OF INTERNAL CONTROL

Issued September 2009

## Table Of Contents

- I. [Preface](#)
- II. [Objective](#)
- III. [Scope](#)
- IV. [Process](#)
- V. [Responsibility](#)
- VI. [Fraud](#)
- VII. [Revisions](#)
  - [Introduction](#)
- 1.0 [General Control Requirements](#)
  - [Quick Reference](#)
- 2.0 [Revenue Cycle](#)
  - 2.1 [Order Entry/Edit](#)
  - 2.2 [Loan/Financial Aid](#)
  - 2.3 [Billing](#)
  - 2.4 [Accounts Receivable](#)
  - 2.5 [Collection](#)
  - 2.6 [Cash Receipts](#)
- 3.0 [Procurement Cycle](#)
  - 3.1 [Supplier Selection and Retention](#)
  - 3.2 [Purchasing](#)
  - 3.3 [Receiving](#)
  - 3.4 [Accounts Payable](#)
  - 3.5 [Disbursements](#)
- 4.0 [Payroll Cycle](#)
  - 4.1 [Human Resources, Compensation, and Benefits](#)
  - 4.2 [Payroll Preparation and Security](#)
  - 4.3 [Payroll Disbursement Controls](#)
  - 4.4 [Distribution of Payroll](#)
- 5.0 [Financial Reporting Cycle](#)
  - 5.1 [Accumulation of Financial Information](#)
  - 5.2 [Processing and Reporting of Financial Information](#)
  - 5.3 [Related Party Accounts](#)

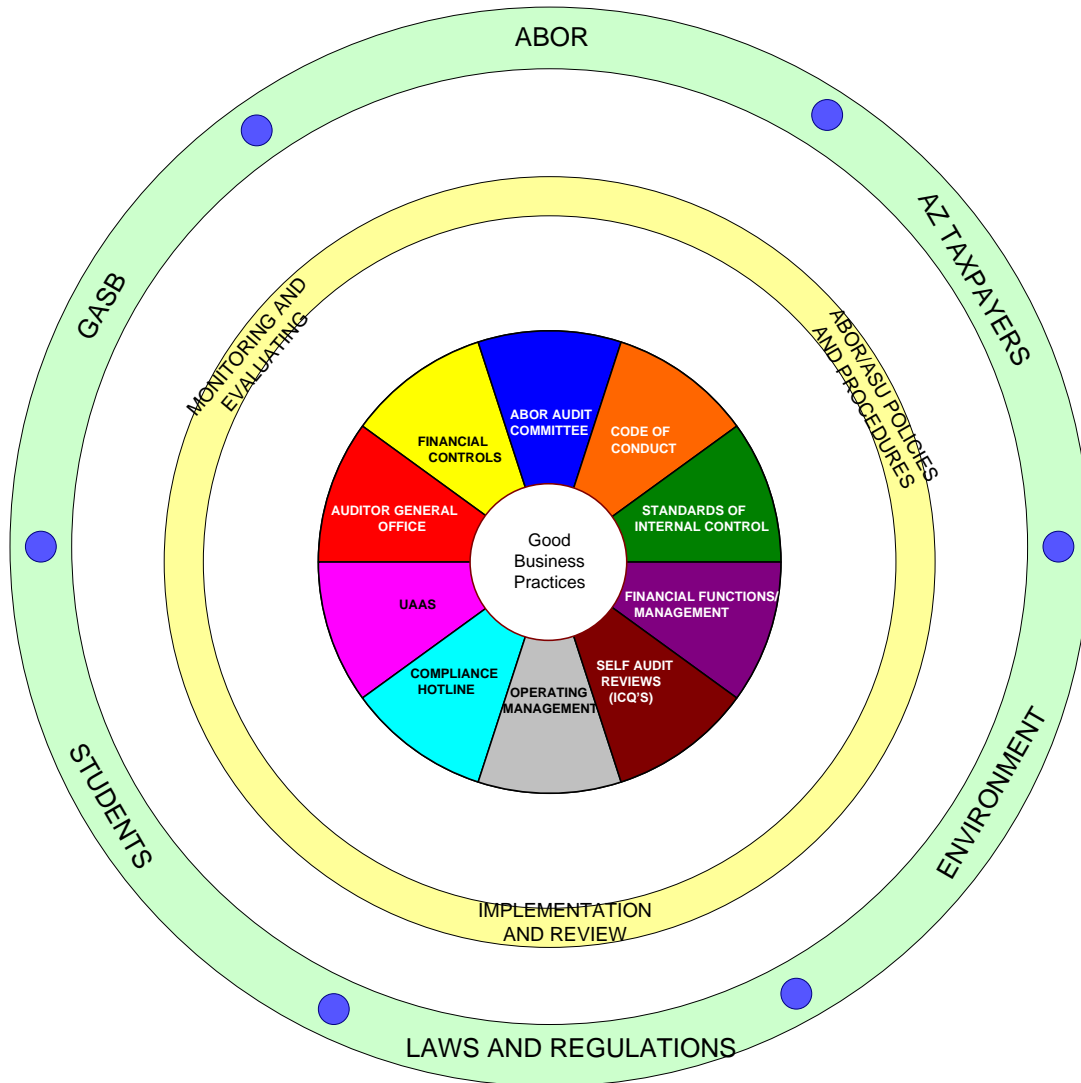
- 6.0 [Computer Systems Controls](#)
  - 6.1 [System Owners and Custodians of Equipment](#)
  - 6.2 [Physical Security and Environmental Controls](#)
  - 6.3 [Computer Access Security](#)
  - 6.4 [Network Security](#)
  - 6.5 [Systems Development Methodology](#)
  - 6.6 [Configuration Management](#)
  - 6.7 [Computer Operations and Back-up](#)
  - 6.8 [Disaster Recovery Planning](#)
  - 6.9 [Input Controls](#)
  - 6.10 [Processing Controls](#)
  - 6.11 [Output Controls](#)
  - 6.12 [Paperless Transaction Processing](#)
- 7.0 [Environment, Health and Safety](#)
- 8.0 [Miscellaneous Cycles](#)
  - 8.1 [Capital Assets](#)
  - 8.2 Subsequent Additions/Future Use
- 9.0 [Loss Prevention Cycle](#)
  - 9.1 [Physical Security](#)
  - 9.2 [Access Controls](#)
  - 9.3 [Personnel Security](#)
  - 9.4 [Physical Asset Protection](#)
  - 9.5 [Protection of Trademarks/Logos](#)
- 10.0 [Intellectual Property](#)

**Acknowledgement:**

The model used within this document is based off that of Motorola, Inc and is being used with their permission. Further refinements to suit the State of Arizona University System were made by Arizona State University.

# I. PREFACE

Our university has long had a formal statement of policy regarding the maintenance of an adequate system of operating and financial controls. The Standards of Internal Control (SIC) were developed to serve as a resource to help document our continued commitment to compliance with applicable university and Arizona Board of Regents' (ABOR) policies/procedures, local, state and federal laws and regulations, reliable operational and financial reporting, and integrity of our activities and records. An overview of our "System of Internal Control" and the external environment it relates to is provided below.



This represents the first edition of the SIC, which was published to help ensure we meet the control requirements necessitated by the ever-changing environments in which we operate. It is based on the Internal Control Standards published by Motorola, Inc., and is used with their permission.

## **II. OBJECTIVE**

Good internal controls are fundamental to achieving our key initiatives and goals. Utilizing good controls as included in this document can help eliminate bottlenecks, redundancies, and unnecessary steps. Controls can prevent loss of resources, including capital assets, inventory, proprietary information, and cash. They can help ensure compliance with applicable laws and regulations. Periodic audits against the control guidelines can ensure that a process in control stays in control.

The objective of this document is to provide a resource to our citizenry that will help assure the existence of basic and consistent internal controls throughout the university. This initial edition of the Standards of Internal Control is the product of the continued efforts of numerous associates in various functions throughout the university. The control criteria included were written in a manner to satisfy the basic objectives of our system of internal control. This system recognizes the need to comply with the expectations of our students, alumni, vendors, faculty/staff and our community. The Audit Committee of the Arizona Board of Regents, the State of Arizona Office of the Auditor General, Internal Audit (IA), the Financial Controls division of the Comptroller's Office and each Business Administrator (BA) across the university are responsible for monitoring our adherence to these standards.

## **III. SCOPE**

These standards are applicable to all campuses, colleges, services and departments. The standards generally reflect control objectives and do not attempt to describe the specific techniques required in each area.

These internal controls are designed to provide reasonable, but not absolute, assurance regarding the safeguarding of resources, reliability of operating and financial information, and compliance with laws and regulations. The concept of reasonable assurance recognizes that the cost of a control should not exceed the benefit to be derived. It also recognizes the need for uncompromising integrity, good business judgment, and a culture of good control practices.

In management's selection of procedures and techniques of control, the degree of control employed is a matter of reasonable judgment. When it may be impractical or impossible to institute any of the controls listed, as could be the case of a small or remote operation/department, management should choose among the following alternatives:

- Improve existing controls through increased supervision and audits;
- Institute alternative or compensating controls; and/or
- Accept the risks inherent with the control weakness.

## **IV. PROCESS**

The controls in this document should not, as indicated by the internal control wheel, be considered to be "stand alone". Together, Internal Control Standards, university policy and procedures manuals, and departmental rules should be considered part of the process for installing, maintaining, and improving our system of internal control.

The internal control process should be supported by a commitment from all levels of the university. The process itself should include operational analysis, development of control procedures and techniques, communication, and monitoring. Operational analysis requires evaluation of risks and a determination of the appropriate control objectives. Also, the operating environment (such as level of automation, budget and resources) should be taken into consideration as well as a cost-benefit analysis to ensure the cost of a control does not exceed its benefit.

Based on the operational analysis, specific control techniques or procedures can be selected. These may include approvals, authorizations, reconciliations, duty segregation, reviews and/or documentation. Throughout the process, communication should flow freely in the form of training, awareness and feedback. Once in place, the control activities should be monitored and evaluated. This can be accomplished through some combination of self audits, internal audits, and external audits. The feedback provided can be used to further improve the internal control system.

## **V. RESPONSIBILITY**

All of us are responsible for compliance with university and ABOR policies and procedures. Each member of upper management is specifically responsible to "set the tone at the top" necessary to establish the proper environment for internal control compliance. They should ensure that the spirit of the control guidelines presented in this manual are established, properly documented and maintained within their organization. Business Administrators and departmental management are responsible for detecting improprieties. Each Business Administrator should be familiar with the types of improprieties which might occur in his/her area and be alert for any indication that a defalcation, misappropriation or irregularity is or was in existence in his/her area. Compliance with the spirit of these standards will be monitored by periodic Internal Audit or Financial Controls reviews (and self-audit reviews, where possible). Each BA will be held accountable for the functioning of the internal control system in their area.

## **VI. FRAUD**

Fraud is the intentional theft, diversion, or misappropriation of university assets. These assets include, but are not limited to; cash, equipment, supplies, salvage, service and software and intellectual property. Fraud may be committed by employees, customers, vendors or others. Studies have shown that organizations have lost between .05 and 2 percent of revenues to fraud. Most incidents or reported frauds have been committed by trusted associates. Fraudulent behavior has been linked with perceived opportunity and rationalization that such behavior is acceptable.

Fraud may also occur in the recording or reporting of university records. Applying the definition of fraudulent reporting as stated by the National Commission on Fraudulent Financial Reporting to the university environment would read similar to the following:

Fraudulent financial reporting is the intentional or reckless conduct, whether by act or omission, that results in material misleading financial statements. Fraudulent financial reporting can involve many factors and take many forms. It may entail gross and deliberate distortion of records, such as inventory counts, or falsified transactions, such as fictitious sales or orders. It may entail the misapplications of accounting principles. Associates at any level may be involved, from senior management to lower-level personnel.

## **Fraud Deterrence/Prevention**

Every manager has a duty to provide a control structure and environment that will protect employees, vendors, students and others from being placed in a position where they will have both the method and opportunity to commit a fraud. Management has established a framework to protect the university from opportunities for fraud by the promotion of internal controls as good business practices. The framework includes resource materials (such as this) provided by Financial Controls, university policy and procedures manuals, and common sense.

## **Fraud Detection and Reporting**

Every member of the university community has a duty to aid in preventing fraud. If an employee identifies situations where fraud might occur, they should report those situations to management. If one suspects that a fraud has taken place, the employee should report the situation to their management, Internal Audit or Financial Controls. All incidents of actual fraud should be reported to the ABOR Audit Committee through the appropriate channel.

Employees should not attempt personal investigations of suspected incidents of fraud. Investigation will be conducted by members of one or more of the following: Internal Audit, Financial Controls, ABOR, General Counsel and/or Office of the Auditor General, and/or the university's police department.

## **VII. REVISIONS**

Revisions will be made to the Standards of Internal Control as required. Proposals for change should be communicated to the Financial Controls division of the Comptroller's Office.

# STANDARDS OF INTERNAL CONTROL

## Introduction

The basic control objectives in this document have been divided into a business cycle format for ease of implementation, reference, and subsequent evaluation. A cycle of a business has been defined as a series of related events or processes. Frequently, a cycle encompasses a specific transaction from its initiation through to completion. For example, the disbursement cycle of a university might encompass requesting a product, creating and approving a purchase order, receiving product and invoice from the vendor and issuing payment to the vendor.

The control guidelines within each cycle have been written in a manner to satisfy the basic objectives of our systems of internal control and to meet external requirements, including Generally Accepted Accounting Principles (GAAP) and applicable laws and regulations. Fundamental control criteria, however, are:

- (i) That transactions are conducted in accordance with management's general or specific AUTHORIZATIONS;
- (ii) That transactions are properly ACCOUNTED for and accurately and promptly RECORDED; and
- (iii) That the assets and records of the university are adequately SAFEGUARDED.

The control matrix shown below provides a general guideline for the processing of all transactions consistent with the control criteria noted above.

## CONTROL MATRIX

Objectives	Input	Process	Output
<b>Authorization</b>	Is the source authorized?	Are the procedures approved?	Is it what was approved?
<b>Recording</b>	Is it accurate/complete? Is it timely? Is it documented?	Who does it? When? Are procedures followed? Is it recoverable? Is management review adequate?	Is it accurate and complete? Is there an audit trail? Is management review adequate? Does it balance?
<b>Safeguarding/Security</b>	Who should control? Are duties separated?	Who can access it? Are duties separated?	Is it confidential? Who should have it?
<b>Verification</b>	Are sources proper?	Are procedures followed complete? Are investigation and review of differences adequate?	Are differences properly resolved? Is management review adequate?

## **1.0 GENERAL CONTROL REQUIREMENTS**

The following general control objectives, which apply to all business cycles, should be adopted by all university operations.

### **Standard of Internal Control**

- 1.1** All employees should comply with all university, ABOR, and departmental policies and procedures, as well as with all local, state and federal laws.
- 1.2** University policy and procedure manuals should be adhered to by all affected organizations. Policies and procedures established within our operating units should, at a minimum, meet and not be in conflict with, the control requirements specified by university policy. Policies and procedures should be periodically reviewed and updated.
- 1.3** Adequate segregation of duties and control responsibilities should be established and maintained in all functional areas of the university. In general, custodial, processing/operating and accounting responsibilities should be separated to promote independent review and evaluation of university operations. Where adequate segregation cannot be achieved, other compensating controls should be established and documented.
- 1.4** No person shall, directly or indirectly, falsify or cause to be falsified any books, records, or accounts of the university.
- 1.5** All departments should develop a system of internal controls to ensure that the assets and records of the university are adequately protected from loss, destruction, theft, alteration or unauthorized access.
- 1.6** Records of the university should be maintained in compliance with established and approved record retention policies.
- 1.7** Costs and expenses of all operating units should be maintained under budgetary control. Comparisons of actual expenses to budgeted amounts should be performed on a regular basis with all significant variances researched.
- 1.8** Employees should be instructed regarding the sensitivity/confidentiality of university information and refrain from unauthorized disclosure of such information to individuals outside the university or to university employees without the "need to know". Adequate security should also be maintained in disposing of confidential/proprietary information.
- 1.9** All operating units and facilities should develop procedures for documenting and reporting to operating management any occurrences of fraud, embezzlement or unlawful or unethical practices. Reports on all significant occurrences should be forwarded to Internal Audit, Financial Controls and/or General Counsel.
- 1.10** Critical transactions in the university's business cycles should be traceable, authorized, authenticated, have integrity and be retained in accordance with established and approved record retention policy.



## STANDARDS OF INTERNAL CONTROL QUICK REFERENCE

**NOTE:** A *preventive* control helps to stop an adverse action from occurring; a *detective* control can catch an adverse action or violation after it has happened. Remember, at least two sets of eyes should be involved in every action that impacts the financial standing or reporting of the university.

<u>CONTROL</u>	<u>LOWERS RISK OF:</u>
<p style="text-align: center;">Segregation of duties: (preventive)</p> <p>No one person should be able to initiate, approve and record a transaction, reconcile the account affected, handle the assets from that transaction, and review reports that would capture that information</p>	<p>Cash misappropriation, financial reporting misstatement, personal purchases, theft, falsification of time and financial records, funds diversion, timing differences across accounting periods</p>
<p style="text-align: center;">Approval/Authorization/Verification: (preventive)</p> <p>Generally, transactions that obligate the university, are over a certain dollar amount, or that impact someone's employment status must be approved by the appropriate level of management</p>	<p>Unauthorized transactions, obligating the university to an unwanted financial or performance commitment, financial reporting misstatement, funds diversion, personal purchases</p>
<p style="text-align: center;">Security/Safeguarding: (preventive and detective)</p> <p>University assets, information, citizens and property should be protected from harm, damage, theft and destruction through locks, passwords, vigilance, monitoring, common sense and communication</p>	<p>Theft, damage, injury, death, financial loss, negative publicity, adverse legal action, compromise of confidential and/or research information</p>

<u>CONTROL</u>	<u>LOWERS RISK OF:</u>
<p style="text-align: center;">Information Technology Controls: (preventive and detective)</p> <p>General controls cover data center operations, software licensing, security access and system maintenance. Application controls cover edit checks and matching/batch processing to help ensure accuracy of information, authorization and validity of transactions</p>	<p>Violation of licensing agreements, fines and penalties, compromise of confidential and/or research information, financial reporting misstatement, adverse legal action, loss of public trust</p>
<p style="text-align: center;">Regular Reconciliations: (detective)</p> <p>In a timely manner, verifies subsidiary information to the official book of record (the university's financial system is the official record for all financial transactions) and helps identify variations from budget</p>	<p>Financial reporting misstatement, making decisions based on erroneous information, personal or prohibited purchases (p-card statement reviews), incorrect payments, account deficits</p>
<p style="text-align: center;">Other controls:</p> <p>Cross-training, job/task rotations, vacations, surprise audits, requesting reviews from independent parties (like the Dean's Office or Financial Controls) or peer groups, asking employees what is working or not working, being involved, following the rules and taking appropriate action when rules/policies are not followed</p>	<p>Low employee morale, losing sleep, being stressed, doing things inefficiently or ineffectively, lagging behind, violating policy, disciplinary action, department turnover and time/money spent posting, hiring and training</p>

**NOTE:** Particular attention should be paid to management override of controls. Repeated policy exceptions or overrides may indicate potential fraudulent activity or a need to reassess current policies/procedures. Any unusual conditions that are identified should be investigated by the appropriate party and include corrective action if necessary. Exceptions to university policy can **only** be approved by the custodian of the relevant policy (e.g. Financial Services, Purchasing, Human Resources, etc. – not each individual department, Dean's Office or VP area).

---

## 2.0 REVENUE CYCLE

The Revenue Cycle includes the functions of acquiring and accepting Sponsored Research monies, donations/gifts, local or state funds, tuition and/or loan monies from students; granting credit; maintaining and monitoring accounts receivable; instituting effective collection procedures; recording and controlling cash receipts; and properly valuing receivable balances.

In management's selection of procedures and techniques of control, the degree of control implemented is a matter of reasonable business judgment. The common guideline that should be used in determining the degree of internal controls implementation is that the cost of a control should not exceed the benefit derived. The specific functions or departments included in the Revenue Cycle are:

[2.1 Order Entry/Edit](#)    [2.4 Accounts Receivable](#)

[2.2 Load/Financial Aid](#)   [2.5 Collection](#)

[2.3 Billing](#)                      [2.6 Cash Receipts](#)

### 2.1 ORDER ENTRY/EDIT

	<u>Standard of Internal Control</u>		<u>Risk if Standard is Not Achieved</u>
2.1.1	Students should be recorded only on the basis of admittance to the university. There should be evidence of the student's initiation of the admissions process, and registration for applicable classes. <i>Refer to risks: A-1, A-2</i>	A-1	Student tuition bill may be shipped without a valid student commitment to the university.
2.1.2	New students and vendors should be processed in appropriate system(s). <i>Refer to risk: A-3</i>	A-2	The student tuition bill may be incorrect.
2.1.3	New students should be processed into the system before registration begins. <i>Refer to risk: A-4</i>	A-3	Registration may be submitted to an unauthorized student resulting in uncollectible accounts.
2.1.4	Formal acknowledgment of the student class schedule should be sent to the student on a timely basis, unless reasonable business practice dictates otherwise. <i>Refer to risk: A-5</i>	A-4	Student registration may be inconsistent with student major resulting in registering for unauthorized classes.
2.1.5	Registration requests should be properly documented. Items to be reviewed include existence of students in the system, student eligibility, etc. <i>Refer to risks: A-1, A-2, A-3, A-6</i>	A-5	Errors in student registration may not be identified or corrected prior to beginning of classes.
2.1.6	ABOR approval is required for any discounts or allowances as defined by university policies. <i>Refer to risk: A-6</i>	A-6	Student tuition discount may be accepted and processed at rates that are unacceptable to ABOR.
2.1.7	Student information should be safeguarded from unauthorized access. <i>Refer to risk: A-7</i>	A-7	Student information may be lost, destroyed, or altered. Confidential information may be used to the detriment of the university or student.

- |       |  |     |   |
|-------|--|-----|---|
| 2.1.8 | Open accounts receivable should be reviewed periodically for outstanding tuition, bills, fees, etc. Any outstanding fees should be researched and resolved.<br><i>Refer to risk: A-8</i> | A-8 | Overdue bills/payments may not be identified, resulting in dissatisfied students or class cancellation. |
|-------|--|-----|---|

## 2.2 LOAN/FINANCIAL AID

- |       | <u>Standard of Internal Control</u>  |     | <u>Risk if Standard is Not Achieved</u>   |
|-------|--|-----|---|
| 2.2.1 | Formal, written loan or financial aid procedures should be established within the university and should be reviewed and approved by ABOR.<br><i>Refer to risks: B-1, B-2</i>   | B-1 | Inconsistent loan or financial aid reviews may be completed.  |
| 2.2.2 | Financial aid or loan limits may be established for each student. Limits should be maintained on the student records and should be based on review of the student's ability to pay. Reliable outside sources of information should be used to establish such loan limits.<br><i>Refer to risk: B-2</i> | B-2 | Financial aid or loans may be given to an unauthorized student resulting in uncollectible accounts. |
| 2.2.3 | A review of approved financial aid or loans and the current receivable balance should be made before additional aids or loans are accepted. Federal government approval is required before student loans are extended in excess of approved limits.<br><i>Refer to risk: B-2</i>                       |     |   |
| 2.2.4 | Established student loan amounts should be reviewed for adequacy at least annually. Where appropriate, adjustments to loan amounts should be made and approved by federal government.<br><i>Refer to risk: B-2</i>   |     |   |

## 2.3 BILLING

- |       | <u>Standard of Internal Control</u>  |     | <u>Risk if Standard is Not Achieved</u>  |
|-------|--|-----|--|
| 2.3.1 | Accountability for tuition bills are the responsibility of the Registrar/Student Business Services (SBS) and may not be delegated to any other functional area. Where invoices are computer generated, SBS should ensure adequate controls exist over invoice preparation.<br><i>Refer to risks: C-1, C-2, C-3</i> | C-1 | Tuition bills may be incorrectly prepared, and/or billings and other terms may be misstated. |

2.3.2	A tuition bill should be prepared on the basis of supporting information about credit hours taken. <i>Refer to risks: C-1, C-2, C-4, C-5</i>	C-2	Tuition bills may have occurred but may not have been billed and/or recorded.
2.3.3	Procedures should be established to ensure that all credit hours have been billed and exceptions promptly resolved. <i>Refer to risks: C-2, C-3, C-4</i>	C-3	Intentional errors or misappropriation of information could occur. Examples include the following:  a. Additional fees may be applied to the bill  b. Tuition may be billed but not recorded in the accounting records.
2.3.4	Sufficient reviews or computer edits should exist to ensure accuracy of invoices recorded and that revenue is recognized in the appropriate accounting period. <i>Refer to risks: C-1, C-2, C-4</i>	C-4	Revenues and expenses may be incorrectly recorded and/or recorded in the wrong accounting period.
2.3.5	Items billed should never be misrepresented. <i>Refer to risk: C-4</i>	C-5	Cash flow may not be maximized due to untimely billings, and the account may become non-collectible.
2.3.6	Appropriate cutoff procedures should be established to ensure the propriety of revenue recorded. <i>Refer to risk: C-4</i>	C-6	Credit transactions may not reflect the proper accounting treatment or may conflict with good business practices.
2.3.7	All credit memos issued to students should be supported by documentation and approved by the Comptroller's Office prior to issuance. <i>Refer to risks: C-3, C-6</i>	C-7	All credit transactions may not be included in the accounting records.
2.3.8	Credit memo transactions should be numerically controlled and accounted for periodically. Credit memos should be pre-numbered where the integrity of sequencing is not computer controlled. <i>Refer to risks: C-4, C-7</i>	C-8	Unauthorized use of the documents may occur resulting in a loss of revenues or an adverse affect on our reputation.
2.3.9	Blank invoice and credit memo stock should be safeguarded. <i>Refer to risk: C-8</i>		
2.3.10	Revenues should be recognized when earned in accordance with Generally Accepted Accounting Principles. <i>Refer to risks: C-4, C-5</i>		

## 2.4 ACCOUNTS RECEIVABLE

	<u>Standard of Internal Control</u>		<u>Risk if Standard is Not Achieved</u>
2.4.1	Accounts receivable records should be maintained by an individual who does not have access to billing documentation or cash remittances. <i>Refer to risk: D-1</i>	D-1	Intentional errors or misappropriation of assets could occur. Examples include:  a. Sales are invoiced but not recorded. Upon receipt, cash is misappropriated.  b. Cash receipts are incorrectly applied to customer accounts and/or are misappropriated or diverted.
2.4.2	Input to the detailed accounts receivable subsidiary ledger should be based upon verified billing records and remittances. Procedures should be established to ensure the accurate and timely recording of billings and payments. <i>Refer to risks: D-2, D-3, D-6</i>	D-2	The subsidiary ledger may be inaccurate as invoices and/or cash receipts may not be recorded, may be incorrectly recorded, or may be recorded in the wrong accounting period.
2.4.3	The detailed accounts receivable subsidiary ledger should be reconciled to the general ledger monthly and any differences appropriately resolved. The reconciliation should be approved by the next level of supervisory accounting. <i>Refer to risks: D-4, D-6</i>	D-3	Inefficient collection activities may occur, and/or incorrect agings may result in delinquent customer remittances or the write-off of delinquent accounts.
2.4.4	An aging of the accounts receivable detail should be reviewed by financial management for any unusual or seriously delinquent items. The aging should be accurate and not distorted by liabilities (e.g., cash with order, down payments, or unapplied cash or credits). <i>Refer to risks: D-3, D-5</i>	D-4	Errors in either the general or subsidiary ledgers may not be identified and corrected on a timely basis.
2.4.5	A system of internal receivable management reporting should be adopted. The internal reports or files could include receivable turnover, aging of accounts, listing of delinquent accounts, potential write-offs, adequacy of collection efforts, etc. <i>Refer to risk: D-3</i>	D-5	The accounts receivable valuation reserves may be incorrectly calculated. Net receivables and the related financial statements may be misstated.
2.4.6	All adjustments to the receivable balances (e.g., credit memos, discounts, account write-offs, debit memos) should be approved in accordance with ABOR/university policy and recorded in the accounting period in which the need for the adjustment was determined. Known receivable adjustments should never be delayed or deferred. <i>Refer to risks: D-6, D-7, D-8</i>	D-6	The financial records and financial statements may be misstated.

2.4.7	Management should develop an accounts receivable valuation reserve policy to state receivables at their net realizable value. The policy should provide for a bad debt reserve and, where appropriate, a billing adjustment reserve. <i>Refer to risk: D-5</i>	D-7	Adjustments processed may not reflect good business practices, or adjustment errors may not be detected.
2.4.8	Valuation reserves should be reviewed at least quarterly for adequacy and reasonableness, and adjustments made as required. <i>Refer to risk: D-5</i>	D-8	Collectible accounts receivable may be written off, and/or cash receipts may be misappropriated.
2.4.9	Detailed accounts receivable information should be safeguarded from loss, destruction, or unauthorized access. <i>Refer to risks: D-9, D-10</i>	D-9	Loss, destruction, or alteration of accounts receivable records may result in the inability to collect outstanding balances.
2.4.10	Records and an aging of accounts receivable from employees, including travel advances, should be maintained independently from the student accounts receivable ledger and should be reviewed and reconciled on a monthly basis. <i>Refer to risks: D-3, D-4, D-6, D-11</i>	D-10	Unauthorized use of customer receivable information could adversely affect our financial position or reputation.
		D-11	Receivables may not be collected from terminated employees.

## **2.5 COLLECTION**

	<b><u>Standard of Internal Control</u></b>		<b><u>Risk if Standard is Not Achieved</u></b>
2.5.1	Formal, written collection procedures should be developed and implemented by management. These procedures should be reviewed and approved by the Comptroller's Office. <i>Refer to risk: E-1</i>	E-1	Inadequate or inconsistent collection policies and procedures may be implemented which could result in inadequate/inefficient collection efforts.
2.5.2	Collections should review the accounts receivable balances (both debits and credits) regularly and initiate collection efforts on all accounts outstanding over the specified number of days. Collection efforts should be adequately documented in the files. <i>Refer to risks: E-2, E-3</i>	E-2	Delinquent accounts may have to be written off due to inadequate collection efforts.
2.5.3	Student correspondence (billing/shipping complaints, service problems, etc.) should be investigated and resolved timely. <i>Refer to risks: E-3, E-4</i>	E-3	Misapplication or misappropriation of cash receipts may not be identified and corrected timely.

- |       |   |     |   |
|-------|---|-----|---|
| 2.5.4 | Student account write-offs should be adequately documented and approved in accordance with policy.<br><i>Refer to risks: E-3, E-4</i> | E-4 | Student dissatisfaction may result in loss of the customer. |
|-------|---|-----|---|

## 2.6 CASH RECEIPTS

- | <u>Standard of Internal Control</u> |  | <u>Risk if Standard is Not Achieved</u> |  |
|-------------------------------------|--|---|--|
| 2.6.1                               | All cash receipts should be restrictively endorsed and secured immediately upon receipt.<br><i>Refer to risk: F-1</i>  | F-1                                     | Cash receipts may be lost and/or misappropriated.  |
| 2.6.2                               | Cash receipts should be logged and deposited in the bank daily or as dictated by policy. The cash receipts log should be compared to bank statements and posted to the general ledger monthly.<br><i>Refer to risks: F-2, F-3</i>  | F-2                                     | Lost, incorrectly recorded, and/or misappropriated cash receipts may not be identified and corrected timely.                 |
| 2.6.3                               | Where good business practice allows, control and responsibility for receiving and depositing checks/cash should be assigned to an individual who is not responsible for: <ul style="list-style-type: none"> <li>a. Recording to the accounts receivable subsidiary ledger;</li> <li>b. Recording to the general ledger;</li> <li>c. Collecting delinquent receivables;</li> <li>d. Authorizing write-offs, credit memos, and discounts</li> <li>e. Preparing billing documents.<br/><i>Refer to risks: F-1, F-2</i></li> </ul> | F-3                                     | Cash flow may not be maximized.  |
| 2.6.4                               | All departments should remit payments directly to Cashiering or via armored car agreement.<br><i>Refer to risks: F-1, F-3</i>  | F-4                                     | Inefficient collection activities may occur due to inaccurate customer account balances.                                     |
| 2.6.5                               | All customer remittances should be promptly reflected in the accounts receivable subsidiary records and specific customer accounts. Unidentified remittances should be promptly investigated and resolved.<br><i>Refer to risks: F-2, F-4, F-5, F-6</i>  | F-5                                     | The receivable balance and/or aging of receivables included in internal receivable management reporting may not be accurate. |
| 2.6.6                               | Monthly customer remittance cutoff procedures should be established.<br><i>Refer to risks: F-5, F-6</i>  | F-6                                     | The financial records and financial statements may be misstated.   |



## 3.0 PROCUREMENT CYCLE

The Procurement Cycle includes the functions of securing and qualifying sources of supply; initiating requests for materials, equipment, supplies, or services; obtaining information as to availability and pricing from approved suppliers; placing orders for goods or services; receiving and inspecting or otherwise accepting the material or service; accounting for the proper amounts owed to suppliers; and processing payments in a controlled and efficient manner.

In management's selection of procedures and techniques of control, the degree of control implemented is a matter of reasonable business judgment. The common guideline that should be used in determining the degree of internal controls implementation is that the cost of a control should not exceed the benefit derived. The specific functions or departments included in the "Procurement" Cycle are:

### 3.1 Supplier Selection and Retention

#### 3.2 Purchasing

#### 3.3 Receiving

#### 3.4 Accounts Payable

#### 3.5 Disbursements

## 3.1 SUPPLIER SELECTION AND RETENTION

	<b><u>Standard of Internal Control</u></b>		<b><u>Risk if Standard is Not Achieved</u></b>
3.1.1	An approved supplier selection/ qualification process should be established in accordance with university policy. University policy should define the involvement of Purchasing, Comptroller's Office, and ethics/diversity in the vendor selection process. Responsibility for supplier selection should not reside with the purchasing department or buyer exclusively. Supplier selection/ qualification responsibility should be segregated from disbursement and accounting activities. <i>Refer to risks: A-1, A-2, A-3</i>	A-1	A purchase may be:  a. Unauthorized or improperly authorized.  b. Made from an unauthorized supplier.  c. Ordered and received by an unauthorized individual.
3.1.2	All criteria used in the supplier selection/ qualification process should be documented and safeguarded. <i>Refer to risks: A-1 through A-6</i>	A-2	Sensitive payments, related party transactions, or conflict of interest situations may occur. The potential for errors and irregularities is substantially increased.
3.1.3	An approved supplier list/database should be established in accordance with policy. The supplier list/database should be continually reviewed, updated, and purged of inactive suppliers. Suppliers should be added to the supplier list/database upon completion of supplier selection process and financial validation. <i>Refer to risks: A-1, A-2, A-3</i>	A-3	Goods purchased may not meet quality standards. Unauthorized prices or terms may be accepted.

- 3.1.4 Where a decision, based on sourcing policy, is made to use sole or single sources of supply for a product or commodity, the justification should be documented, approved, and retained in accordance with policy. For sources where a disruption of supply may have significant negative consequences to the university, a business interruption plan should be established, documented, and approved in order to ensure adequate supply of material during emergencies. A sole source of supply situation exists whenever a given product/material can be purchased from only one supplier. A single source of supply situation exists when several suppliers are capable of providing products or materials but only one supplier is used.  
*Refer to risks: A-2, A-3, A-6*
- 3.1.5 Suppliers should be periodically monitored in accordance with university policy to ensure that actual performance meets expectations. Performance reporting may include:
- a. Percent of on-time delivery;
  - b. Accuracy of shipments;
  - c. Product quality; and
  - d. Departments should calculate actual costs as compared to previous year or formula/target costs.  
*Refer to risks: A-1, A-2, A-3, A-6*
- A-4 Records may be lost or destroyed.
- A-5 Records may be misused or altered by unauthorized personnel to the detriment of the university and its suppliers.
- A-6 Materials may be received early or late resulting in business interruption or excessive levels of inventory.

## **3.2 PURCHASING**

	<b><u>Standard of Internal Control</u></b>		<b><u>Risk if Standard is Not Achieved</u></b>
3.2.1	All purchasing responsibilities should be segregated from disbursement and accounting activities. <i>Refer to risks: B-1, B-2</i>	B-1	A purchase may be:  a. Unauthorized or improperly authorized.  b. Made from an unauthorized supplier.  c. Ordered and received by an unauthorized individual.
3.2.2	Independence between purchasing agent or buyer and supplier should be maintained. This can be accomplished through periodic buyer rotation, participation in purchase contracts, or the use of commodity teams. Other compensating controls should exist if business conditions make the above impractical. <i>Refer to risks: B-1, B-2</i>	B-2	Sensitive payments, related party transactions, or conflict of interest situations may occur. The potential for errors and irregularities is substantially increased.
3.2.3	Purchase orders are required for merchandise or services purchased as defined by university policy. Purchase orders/requisitions are not always appropriate or required for "one-time" expenditures such as training seminars, professional dues, etc. Where a paperless environment exists, purchase orders/requisitions need not be hard copy but adequate documentation, control authorization and record retention should be addressed. <i>Refer to risks: B-1, B-3, B-4, B-10</i>	B-3	Rather than being returned or refused, the following items may be received and ultimately paid for:  a. Unordered goods or services.  b. Excessive quantities or incorrect items.  c. Canceled or duplicated orders.
3.2.4	Procurement requests should be initiated by the requesting department and be properly approved before a purchase commitment is made. <i>Refer to risks: B-1, B-2</i>	B-4	Records may be lost or destroyed.
3.2.5	All purchase orders/transactions should be uniquely identifiable and traceable and periodically accounted for. <i>Refer to risks: B-5, B-6</i>	B-5	Records may be misused or altered by unauthorized personnel to the detriment of the university and its suppliers.
3.2.6	All purchase orders or access to input screens should be safeguarded and internal control procedures for processing and approval should be in place to prevent unauthorized use. <i>Refer to risks: B-1, B-2, B-4, B-5</i>	B-6	Goods and services may be received but not reported or reported inaccurately. Unrecorded liabilities and misstated costs may occur.

- |        |   |      |  |
|--------|---|------|--|
| 3.2.7  | Purchase orders/transactions should include all pertinent information concerning formal commitments including quantities, delivery means and requirements, payment terms and conditions, account distribution, etc.<br><i>Refer to risks: B-2, B-3, B-7, B-8</i>  | B-7  | Goods purchased may not meet quality standards. Unauthorized prices or terms may be accepted.  |
| 3.2.8  | POs/transactions should instruct suppliers to forward their billings directly to the A/P department.<br><i>Refer to risks: B-1, B-2, B-3, B-5, B-6, B-9</i>   | B-8  | Materials may be received early or late resulting in business interruption or excessive levels of inventory.   |
| 3.2.9  | Competitive bids should be obtained for all purchases over a specified and predetermined amount established by university policy. Absence of competitive bids on commitments, or accepting a price other than the lowest bid for items/services other than those under current agreement should be adequately justified and approved by management before a purchase commitment is made.<br><i>Refer to risks: B-2, B-7</i> | B-9  | Duplicate payments may occur, or payments may be made for the wrong amount or to unauthorized or fictitious suppliers.   |
| 3.2.10 | Purchase orders or their equivalent should be made available to the receiving department for verification of incoming receipts and to the A/P dept. for comparison with supplier billings.<br><i>Refer to risks: B-1, B-3, B-6, B-9, B-12</i>   | B-10 | Records may not be available for external legal, tax, or audit purposes.   |
| 3.2.11 | Purchase order revisions for price or quantity increases in excess of the buyer's authorized approval level should be approved in compliance with policy.<br><i>Refer to risks: B-1, B-7</i>  | B-11 | Purchases and/or disbursements may be recorded at the incorrect amount, to the wrong account, or in the wrong period.  |
| 3.2.12 | A/P should be notified of changed or canceled purchase orders on a timely basis.<br><i>Refer to risks: B-3, B-6, B11, B-12</i>  | B-12 | Payment may be made for goods or services never received.  |
| 3.2.13 | Procedures should be established to ensure proper approval and recording of all capital or expense items which are to be returned to the supplier due to poor quality, improper specifications, etc.<br><i>Refer to risk: B-13</i>  | B-13 | Defective merchandise may be handled negligently, returned inadvertently to inventory, and/or recorded incorrectly. The potential for theft increases substantially. |
| 3.2.14 | Contracts, memorandums of understanding, and letters of intent that financially obligate the university should be approved by management, per policy. General Counsel should also approve these documents unless "boiler plate" format and language previously approved is used.<br><i>Refer to risks: B-1, B-6</i>   |      |  |

### **3.3 RECEIVING**

	<b><u>Standard of Internal Control</u></b>		<b><u>Risk if Standard is Not Achieved</u></b>
3.3.1	The receiving department should be physically segregated from the ordering department unless good business practice dictates otherwise. <i>Refer to risks: C-1, C-2</i>	C-1	A purchase may be:  a. Unauthorized or improperly authorized.  b. Made from an unauthorized supplier.  c. Ordered and received by an unauthorized individual.
3.3.2	Access to the receiving department should be restricted to authorized personnel only. <i>Refer to risks: C-1, C-2</i>	C-2	Sensitive payments, related party transactions, or conflict of interest situations may occur. The potential for errors and irregularities is increased.
3.3.3	All incoming items and supplies should be processed by the designated receiving location at each facility, unless otherwise arranged and approved in accordance with university policy. <i>Refer to risks: C-1, C-2, C-4, C-5</i>	C-3	Rather than being returned or refused, the following items may be received and ultimately paid for:  a. Unordered goods or services.  b. Excessive quantities or incorrect items.  c. Canceled or duplicated orders.
3.3.4	The receiving location will accept only those goods for which an approved purchase order or its equivalent has been prepared. All other receipts should be returned to the supplier or investigated for propriety in a timely manner. <i>Refer to risks: C-3, C-4, C-5</i>	C-4	Records may be lost or destroyed.
3.3.5	Each designated receiving location should account for and provide evidence of a receiving transaction for all items, services or supplies accepted by the receiving location. <i>Refer to risks: C-2, C-6, C-7</i>	C-5	Records may be misused or altered by unauthorized personnel to the detriment of the university and its suppliers.
3.3.6	Receiving transactions will not be generated without actual receipt of goods or services and adequate proof of delivery. <i>Refer to risk: C-6</i>	C-6	Goods and services may be received but not reported or reported inaccurately. Unrecorded liabilities and misstated inventory and cost of sales may occur.
3.3.7	In the absence of an effective supplier qualification and performance monitoring program, incoming goods should be test counted, weighed, or measured on a sample basis to determine the accuracy of supplier's shipments. All count discrepancies should be noted on the receiving transaction and appropriately resolved with the supplier. <i>Refer to risks: C-2, C-3, C-4, C-7</i>	C-7	Goods purchased may not meet quality standards. Unauthorized prices or terms may be accepted.

- 3.3.8 Receiving transaction information should be maintained in the receiving department and made available to Purchasing and A/P for supplier payment processing on a timely basis.  
*Refer to risks: C-2, C-6, C-7* C-8 Materials may be received early or late resulting in business interruption or excessive levels of inventory.
- 3.3.9 In the absence of an effective supplier qualification and performance monitoring program, incoming goods should be promptly inspected and tested for damage, quality characteristics, product specifications, etc.  
*Refer to risks: C-4, C-7* C-9 Purchases and/or disbursements may be recorded at the incorrect amount, to the wrong account, or in the wrong period.
- 3.3.10 Receiving transaction information should be adequately safeguarded from theft, destruction, or unauthorized use. Receiving transactions should be uniquely identifiable, traceable and accounted for periodically.  
*Refer to risks: C-1, C-8, C-9*
- 3.3.11 Incoming goods should be secured and safeguarded upon receipt. Valuable commodities should be safeguarded during the receiving process.  
*Refer to risk: C-1*
- 3.3.12 Changes required to correct errors in original receiving transactions may be generated only by authorized personnel as specified by university policy.  
*Refer to risks: C-1, C-2, C-4, C-7*

## **3.4 ACCOUNTS PAYABLE**

	<b><u>Standard of Internal Control</u></b>		<b><u>Risk if Standard is Not Achieved</u></b>
3.4.1	<p>The accounts payable function should be:</p> <p>a. Segregated from purchasing and receiving activities.</p> <p>b. Segregated from general ledger recording activities within the Accounts Payable Department. <i>Refer to risks: D-1, D-2</i></p>	D-1	<p>Purchases may be stolen, lost, destroyed or temporarily diverted. The potential for errors and irregularities is substantially increased.</p>
3.4.2	<p>Prior to payment, the supplier's invoice or equivalent should be reviewed in accordance with university policy for authorization, receipt of material or services and accuracy of price, quantity and account distribution. The absence of any of the referenced information or discrepancies between the information (e.g., price, quantity, etc.) should be resolved before payment is made. <i>Refer to risks: D-2, D-4, D-7, D-8, D-9</i></p>	D-2	<p>Purchases may be received but never reported, or reported inaccurately. Unrecorded liabilities and misstated inventory and accounts payable may occur.</p>
3.4.3	<p>Invoices for which a purchase order or receiving report does not exist (e.g., check requests, one-time purchases, etc.) should be approved by management in accordance with the university approval authorization limits before payment. <i>Refer to risks: D-2, D-3, D-6, D-7</i></p>	D-3	<p>Purchases or services may be ordered and received by an unauthorized individual.</p>
3.4.4	<p>Freight bills above an established limit as stipulated in policy, should be compared to the supporting shipping or receiving documentation before payment. <i>Refer to risks: D-4, D-6, D-7</i></p>	D-4	<p>Rather than being returned or refused, the following goods or services may be received and ultimately paid for:</p> <p>a. Unordered goods or services.</p> <p>b. Inventory that does not meet quality standards.</p> <p>c. Excessive quantities or incorrect items.</p>
3.4.5	<p>Adequate supporting documentation should be attached or otherwise matched to all invoices processed for payment, including approved expense statements and check requests. Such documentation should be reviewed before an invoice, check request or expense statement is approved for payment. <i>Refer to risks: D-6, D-7</i></p>	D-5	<p>Payment may be made for goods or services not received and/or in advance of receipt.</p>

- |        |   |     |   |
|--------|---|-----|---|
| 3.4.6  | Original invoices should be used as the basis for payment. Where the original invoice is not available, a copy can be used only if it is properly authorized as outlined by university policy.<br><i>Refer to risks: D-5, D-6</i>   | D-6 | Payments to suppliers may be duplicated, incorrect, or fraudulent.  |
| 3.4.7  | Aged, unmatched purchase orders, receiving transactions, and invoices should be periodically reviewed, investigated and resolved.<br><i>Refer to risks: D-2, D-4</i>  | D-7 | Records may be lost or destroyed.   |
| 3.4.8  | Supplier statements should be reviewed on at least a test basis for past due items and resolved in a timely manner.<br><i>Refer to risks: D-2, D-4, D-6, D-8</i>  | D-8 | Records may be misused or altered to the detriment of the university or its suppliers.  |
| 3.4.9  | A trial balance of accounts payable should be accumulated on a monthly basis and reconciled to the general ledger. All differences should be resolved on a timely basis.<br><i>Refer to risks: D-4, D-5</i>   | D-9 | <p>A purchase may be:</p> <ul style="list-style-type: none"> <li>a. Unauthorized or improperly authorized.</li> <li>b. Made from an unauthorized supplier.</li> <li>c. Ordered and received by an unauthorized individual.</li> </ul> |
| 3.4.10 | A/P should review debit balance accounts at least quarterly and request remittance on debit amounts outstanding more than 90 days.<br><i>Refer to risk: D-5</i>   |     |   |
| 3.4.11 | Debit and credit memos issued to supplier accounts should be documented and approved in accordance with management authorization listings.<br><i>Refer to risks: D-2, D-5, D-6,</i>   |     |   |
| 3.4.12 | Debit and credit memos should be uniquely identifiable and traceable. Hard copy documents should be easily identifiable and traceable.<br><i>Refer to risks: D-5, D-6</i>   |     |   |
| 3.4.13 | Prior to payment, A/P should ensure the supplier is included on the approved supplier list/database.<br><i>Refer to risks: D-4, D-6</i>   |     |   |
| 3.4.14 | Petty cash transactions should be limited to amounts of a low value and transactions which will not limit the ability to review expenses for reasonableness. Independent confirmations of petty cash funds should be performed periodically.<br><i>Refer to risks: D-5, D-9</i> |     |   |



## 3.5 DISBURSEMENTS

	<u>Standard of Internal Control</u>		<u>Risk if Standard is Not Achieved</u>
3.5.1	<p>The disbursement function should have the following segregation of duties:</p> <p>a. Segregation of payment preparation from check signing and mailing of signed checks;</p> <p>b. Segregation of accounts payable activities from the purchasing and receiving activities;</p> <p>c. Segregation of payment preparation, printing, signing and distribution activity from supplier validation and set-up, and from invoice input activity; and</p> <p>d. Segregation of vendor validation and set-up from invoice input activity and payment preparation and distribution. <i>Refer to risks: E-1, E-2, E-3</i></p>	E-1	Procedures may be implemented that circumvent existing internal control techniques. The potential for theft and error is substantially increased.
3.5.2	<p>All payments should be traceable, uniquely identifiable and accounted for on a periodic basis. <i>Refer to risks: E-1, E-2, E-5</i></p>	E-2	Sensitive payments and related party transactions may occur.
3.5.3	<p>Requests for the preparation of payments should be supported by purchase orders, receiving transactions, original invoices, or their equivalent as required by policy which indicates the propriety of the expenditures. Such documentation will be provided to, and reviewed by, the signers prior to approval. <i>Refer to risks: E-3, E-4, E-5, E-8</i></p>	E-3	Purchases or services may be ordered and received by an unauthorized individual.
3.5.4	<p>Approved payments should be made within the agreed upon terms. <i>Refer to risk: E-9</i></p>	E-4	Items or services may be received but not reported, or reported inaccurately. Unrecorded liabilities, misstated inventories and over/under payments to suppliers may result.
3.5.5	<p>All supplier discounts should be taken if the invoice is paid within purchase order or invoice terms. <i>Refer to risks: E-6, E-10</i></p>	E-5	Duplicate payments may occur, or payments may be made for the wrong amount or to unauthorized or fictitious suppliers.
3.5.6	<p>All disbursements should be properly and accurately recorded in the accounting records during the period in which the liability was incurred or the payment was made. The proper recognition of expense should never be delayed or deferred. <i>Refer to risks: E-4, E-6, E-7, E-10</i></p>	E-6	Financial statements, records, and operating reports may be misstated. Critical decisions may be based upon erroneous information.

- |        |  |      |  |
|--------|--|------|--|
| 3.5.7  | <p>Checks should not be made payable to cash or bearer.<br/><i>Refer to risks: E-1, E-4, E-8</i></p>   | E-7  | <p>Purchases or services may be unauthorized, recorded for the wrong amount or in the wrong period, and/or payment made to the wrong person.</p> |
| 3.5.8  | <p>Blank check stock identifying the university or its financial institutions should be safeguarded from destruction or unauthorized use. The supply of blank checks should be periodically accounted for as being issued, voided or unused. Facsimile signature plates and digitized signature images, where used, should be safeguarded.<br/><i>Refer to risks: E-1, E-4, E-5, E-8</i></p> | E-8  | <p>Items may be recorded and payment made for goods or services not received.</p>  |
| 3.5.9  | <p>Specific limits of signing authority for checks, promissory notes and bank transfers should be established by the President and/or ABOR.<br/><i>Refer to risks: E-1, E-2, E-4, E-8</i></p>  | E-9  | <p>Operations may be adversely affected as suppliers may refuse future business with the university.</p>   |
| 3.5.10 | <p>Dual signatures are required on all manually signed checks/promissory notes issued above the limit specified in policy. At least one of the signers should be independent of invoice approval responsibilities unless good business practice dictates otherwise.<br/><i>Refer to risks: E-1, E-5, E-8</i></p>   | E-10 | <p>Cash utilization may not be optimized or may be misappropriated.</p>  |
| 3.5.11 | <p>In conjunction with system based controls to detect and prevent duplicate payments, supporting documents should be effectively canceled after payment to prevent accidental or intentional reuse.<br/><i>Refer to risks: E-1, E-2, E-5</i></p>  |      |  |
| 3.5.12 | <p>Signed checks should be delivered for mailing to persons independent of invoice processing and maintenance of accounts payable records.<br/><i>Refer to risks: E-1, E-8</i></p>   |      |  |
| 3.5.13 | <p>Spoiled, voided and canceled checks should have the signature portion removed immediately. The checks should be accounted for and protected. The checks may be destroyed, provided destruction is witnessed and documented by an additional individual.<br/><i>Refer to risks: E-1, E-8</i></p>   |      |  |
| 3.5.14 | <p>Documents or electronic data supporting expenditures should be safeguarded from loss or destruction, and should be in a retrievable format.<br/><i>Refer to risk: E-6</i></p>   |      |  |

## 4.0 PAYROLL CYCLE

The Payroll Cycle includes the functions involved in hiring employees and determining their proper classification and compensation; reporting hours worked, attendance, and compensatory absences; preparing payroll checks in a controlled and accurate manner; accurately accounting for payroll costs, deductions, employee benefits, and other adjustments; distributing checks to employees; and ensuring the confidentiality and physical security of payroll and personnel information.

In management's selection of procedures and techniques of control, the degree of control implemented is a matter of reasonable business judgment. The common guideline that should be used in determining the degree of internal controls implementation is that the cost of a control shouldn't exceed the benefit derived.

The term "checks" in this section is generically used to describe all forms (electronic, bank transfer, etc.) of payroll payments to employees. The specific processes included in the Payroll Cycle are:

### 4.1 Human Resources, Compensation, and Benefits

#### 4.2 Payroll Preparation and Security

#### 4.3 Payroll Disbursement Controls

#### 4.4 Distribution of Payroll

## 4.1 HUMAN RESOURCES, COMPENSATION, AND BENEFITS

	<b><u>Standard of Internal Control</u></b>	<b><u>Risk if Standard is Not Achieved</u></b>
4.1.1	Human Resources (HR) management <b>A-1</b> should establish and maintain policies and guidelines for the hiring, promotion, transfer, and termination of employees. The policies and guidelines should be clearly defined by HR management in the form of specific criteria and procedures. <i>Refer to risk: A-1</i>	Individuals may be employed who do not meet our hiring criteria resulting in an inadequate work force in terms of numbers and/or quality.
4.1.2	Policies for major employee benefits, <b>A-2</b> such as sick leave, pension, vacations, and insurance should be reviewed and approved by ABOR. Rules, criteria, procedures, etc. for all benefits should be documented and approved by management. <i>Refer to risks: A-2, A-3, A-4</i>	Incorrect amounts may subsequently be disbursed to employees.
4.1.3	Compensation to employees should <b>A-3</b> be made at appropriate authorized rates and in the proper classifications for the services rendered. Changes to compensation should be properly authorized. Compensation may also take the form of reduced tuition and other rates; such additional compensation should be properly authorized and taxed. <i>Refer to risks: A-2, A-4</i>	Accruals for benefits, pension, vacation and insurance, may be incorrectly calculated, resulting in misstated liabilities.

- |       |   |     |  |
|-------|---|-----|--|
| 4.1.4 | All compensation and benefit documentation should be properly maintained by HR management. HR documentation should, at a minimum, include properly executed employment forms, authorized classification and pay rates.<br><i>Refer to risk: A-4</i>   | A-4 | Laws and governmental regulations may be violated resulting in fines, penalties, lawsuits or contingent liabilities.         |
| 4.1.5 | Formal procedures, along with controlled and approved documents, should be maintained to ensure that only authorized additions, deletions or changes to employee information are allowed. Periodic testing of the permanent payroll records should be performed to ensure that the payroll information agrees with the HR file documentation.<br><i>Refer to risks: A-2, A-4, A-5, A-6, A-8</i>                 | A-5 | Payroll and payroll tax accounts may be misstated.   |
| 4.1.6 | Designated HR management should be responsible for the administration of the employee benefit plans. The plans should be administered in accordance with ABOR policy and defined plan procedures. Benefit payments to employees should be made in accordance with the terms and conditions of the plans and should be adequately documented and properly approved.<br><i>Refer to risks: A-2, A-3, A-4, A-6</i> | A-6 | Unauthorized transactions may be processed resulting in improper disbursements and/or disbursements to fictitious employees. |
| 4.1.7 | Prior to disbursing the final payroll check to a terminated employee, HR and the employee's departmental supervisor should ensure:  | A-7 | Outstanding advances may not be collectible.   |
|       | a. All outstanding advances and expense statements have been cleared;   |     |  |
|       | b. All university credit cards have been returned;  |     |  |
|       | c. All computer accounts have been canceled or passwords changed; and   |     |  |
|       | d. All university property, proprietary information, employee badges, and security passes or keys have been returned.<br><i>Refer to risks: A-7, A-10, A-11</i>   |     |  |

- |       |   |      |  |
|-------|---|------|--|
| 4.1.8 | HR responsibilities, including payroll authorization, should be segregated from payroll distribution and recording responsibilities.<br><i>Refer to risk: A-9</i> | A-8  | Improper disbursements may not be detected and corrected.  |
|       |   | A-9  | Unauthorized transactions may be processed and remain undetected resulting in the misappropriation or temporary diversion of funds.          |
|       |   | A-10 | Unauthorized charges may be incurred subsequent to termination of employment for which the university may become liable.                     |
|       |   | A-11 | Unnecessary computer charges may be incurred, and access to university information by terminated employees may not be adequately restricted. |

## 4.2 PAYROLL PREPARATION AND SECURITY

- | <u>Standard of Internal Control</u> |   | <u>Risk if Standard is Not Achieved</u> |  |
|-------------------------------------|---|---|--|
| 4.2.1                               | A payroll master file should be maintained which includes all employees. The file should contain all information concerning current pay rates, withholding deductions, tax codes, etc.<br><i>Refer to risk: B-1</i>   | B-1                                     | Incorrect information in the payroll master file could result in incorrect payments. Withholdings of earned wages may be incorrect.  |
| 4.2.2                               | Procedures should be established to physically secure and protect master file information. Changes should be restricted to properly authorized additions, deletions and changes which are supported by documentation in the employee's personnel file.<br><i>Refer to risk: B-2</i> | B-2                                     | <p>Inadequate security over the Payroll Department and its records may result in:</p> <p>a. Destruction or loss of payroll records, including the payroll master file;</p> <p>b. Unauthorized review and/or disclosure of confidential payroll information; and/or</p> <p>c. The processing of unauthorized changes to the payroll master file. This, in turn, may result in the following:</p> <ol style="list-style-type: none"> <li>1. Misappropriation of university assets; and</li> <li>2. Misstatement of accruals such as pensions.</li> </ol> |

- |       |   |     |   |
|-------|---|-----|---|
| 4.2.3 | <p>Only authorized personnel should have access to the Payroll department and its records.<br/><i>Refer to risk: B-2</i></p>  | B-3 | <p>Employees may be incorrectly paid or paid for services not received, and collection of overpayments to terminated employees may require legal action. Employee withholdings may also be incorrect.</p> |
| 4.2.4 | <p>The Payroll department should be promptly and formally notified of the termination or transfer of any employee or of payroll changes so that payroll records can be adjusted.<br/><i>Refer to risks: B-3, B-5, B-6</i></p>   | B-4 | <p>Employees may be erroneously paid for hours not worked or may not be paid for hours actually worked. Charges to the wrong department may not be detected.</p>  |
| 4.2.5 | <p>Non-exempt employees are required to submit on a timely basis, time cards, time sheets or other authorized recording media before payroll processing is performed.<br/><i>Refer to risks: B-4, B-6, B-7</i></p>  | B-5 | <p>Management reports and employee earnings records may be inaccurate.</p>  |
| 4.2.6 | <p>Payrolls should be prepared from the payroll master file and the approved time reporting records. Paychecks, payroll registers, and employee earnings records should be prepared simultaneously where feasible. Otherwise, a reconciliation of the payroll earnings records and the payroll (check) register should be completed timely.<br/><i>Refer to risks: B-4, B-5, B-6, B-7</i></p> | B-6 | <p>Unauthorized payments may be made and/or funds may be misappropriated.</p>   |
| 4.2.7 | <p>Controls should be maintained, with sufficient edits, to ensure all payroll source data is valid and properly input. Controls should also be established to ensure duplicate or unauthorized payroll source data may not be processed.<br/><i>Refer to risks: B-5, B-6, B-7, B-8</i></p>   | B-7 | <p>Inaccurate information may be input into the general ledger. The financial statements may be misstated.</p>  |
| 4.2.8 | <p>The appropriate department managers should compare actual payroll costs to budgeted costs for reasonableness.<br/><i>Refer to risk: B-9</i></p>  | B-8 | <p>The processing of payroll may be incomplete and/or inaccurate. There is an increased opportunity for intentional or unintentional processing errors to go undetected.</p>                              |
| 4.2.9 | <p>Payroll withholdings should be controlled to ensure the propriety of amounts, compliance with applicable governmental requirements, timely remittance to the appropriate entity and timely reconciliation to the general ledger accounts.<br/><i>Refer to risks: B-7, B-10, B-12</i></p>   | B-9 | <p>Errors which would not be detected during routine edits (e.g., ineligible or unauthorized employees) may not be detected and corrected.</p>  |

- |        |   |      |  |
|--------|---|------|--|
| 4.2.10 | Departmental procedures should be clearly documented for all major payroll functions and period-end cutoff procedures.<br><i>Refer to risks: B-5, B-7, B-11</i>   | B-10 | Detailed withholdings and payments may not agree to the recorded withholdings and payments.  |
| 4.2.11 | Annual summaries of employee wages and withholdings should be prepared and mailed directly to all employees in accordance with applicable governmental requirements.<br><i>Refer to risk: B-12</i>  | B-11 | Consistent procedures may not be followed resulting in the incorrect, incomplete or untimely processing of payroll information and potential errors in earned wages paid to employees. |
| 4.2.12 | Special payments processed by the Payroll department (e.g., relocations, special engagements for other departments, supp pay, etc.) should be properly authorized, approved, and documented before payment and should be in accordance with applicable tax requirements.<br><i>Refer to risk: B-6</i> | B-12 | Non-compliance and/or calculation errors may result in fines and penalties being assessed by the government.   |
| 4.2.13 | Payroll preparation responsibilities should be segregated whenever feasible from payroll authorization, check signing and check distribution responsibilities. Where segregation is not feasible, compensating controls should be established.<br><i>Refer to risk: B-13</i>                          | B-13 | Unauthorized transactions may be processed and remain undetected resulting in the misappropriation or temporary diversion of assets.   |

### **4.3 PAYROLL DISBURSEMENT CONTROLS**

- |       | <b><u>Standard of Internal Control</u></b>   |     | <b><u>Risk if Standard is Not Achieved</u></b>   |
|-------|--|-----|--|
| 4.3.1 | Payroll disbursements should be drawn on a zero balance bank account. Reimbursement to the account should be equal to net pay for each payroll prepared.<br><i>Refer to risk: C-1</i>  | C-1 | Errors and omissions in the safeguarding, authorization and processing of checks may not be detected and corrected. The financial statements may be misstated. |
| 4.3.2 | All disbursement accounts should be reconciled on a monthly basis.<br><i>Refer to risk: C-1</i>  | C-2 | Checks may be issued which have not been recorded, resulting in incorrect financial statements.  |
| 4.3.3 | All payroll payments should be traceable and uniquely identifiable.<br><i>Refer to risks: C-2, C-3, C-7</i>  | C-3 | Unauthorized use or issuance of payroll checks may occur, and any misappropriation of cash may go undetected.  |
| 4.3.4 | Blank check stock identifying the university or its financial institutions should be pre-numbered and safeguarded. All payroll checks should be periodically accounted for as being issued, voided or unused.<br><i>Refer to risk: C-3</i> | C-4 | Checks may be diverted and cashed by unauthorized persons.   |

- 4.3.5 Spoiled, voided and/or canceled checks should be accounted for and immediately destroyed, provided the destruction is witnessed and documented by an additional individual.  
*Refer to risk: C-3*
- 4.3.6 Signed payroll checks, manual warrants, and direct deposit advices should be secured until distributed to employees.  
*Refer to risks: C-4, C-5*
- 4.3.7 Payroll check signatories should be individuals having no payroll authorization or preparation responsibilities, access to the unused checks or check distribution responsibilities.  
*Refer to risks: C-3, C-4*
- 4.3.8 Completed payroll registers, journal reports and requests for payroll account reimbursement (or similar documents to support the amounts being paid) should be reviewed and approved by appropriate financial management prior to disbursement.  
*Refer to risk: C-6*
- 4.3.9 Formal authorization procedures should be established and adhered to in the signing of payroll checks. Dual signatures are required on all manually signed checks above the limit established by the university.  
*Refer to risk: C-3*
- 4.3.10 Where check signing equipment and facsimile signature plates or digitized signature images are utilized, the equipment and plates should be secured and custody of the check signing equipment and the signature plates or digitized signature image files should be segregated. In addition, reconciliation of checks written should be compared to the check signing machine totals.  
*Refer to risks: C-2, C-3*
- C-5 Confidential payroll information may be reviewed and/or disclosed by unauthorized persons to the detriment of the university or its employees.
- C-6 Significant payroll errors or unauthorized transactions may not be detected prior to payroll distribution.
- C-7 Duplicate check numbers may be assigned or check numbers may be omitted.



## **4.4 DISTRIBUTION OF PAYROLL**

	<b><u>Standard of Internal Control</u></b>		<b><u>Risk if Standard is Not Achieved</u></b>
4.4.1	Persons responsible for the distribution of payroll checks should have no other personnel or payroll responsibilities and should not approve labor hours or time cards. If adequate segregation of duties cannot be achieved, other compensating controls should be established and maintained. <i>Refer to risk: D-1</i>	D-1	Funds may be misappropriated as improper changes/additions could be made to the master file or incorrect hours may be submitted for payment.
4.4.2	Within each facility, signed receipts should be obtained from individuals who receive payroll checks/advices for distribution. <i>Refer to risk: D-2</i>	D-2	An audit trail may not be created to assess responsibility for lost or diverted checks.
4.4.3	Periodic audits should be performed on a test basis by representatives of the appropriate Dean's Office/VP area to positively identify all employees on the payroll. <i>Refer to risk: D-3</i>	D-3	Distribution may be made to unauthorized employees and remain undetected.
4.4.4	Unclaimed or undistributed wages should be returned to HR. Disbursements of unclaimed wages should be made only upon proper employee identification. Unclaimed wages not disbursed in a reasonable timeframe are to be returned to the HR department and should be recorded to a separate unclaimed wages account on the general ledger. Unclaimed wages should be remitted to the appropriate government authorities when required by law. <i>Refer to risk: D-4</i>	D-4	Misappropriation of unclaimed checks, loss of checks, bank statements that can't be reconciled and/or non-compliance with government regulations could result.
4.4.5	The distribution of cash wages is prohibited. <i>Refer to risk: D-5</i>	D-5	Distribution of cash to unauthorized individuals could occur. Also, there may be no evidence if an employee were to allege wages were not paid.
4.4.6	The confidentiality of payroll information should be maintained. <i>Refer to risk: D-6</i>	D-6	Confidential payroll information may be accessed and/or disclosed to the detriment of the university and its employees.

## **5.0 FINANCIAL REPORTING CYCLE**

The Financial Reporting Cycle encompasses the functions involved in ensuring that Generally Accepted Accounting Principles (GAAP) are followed by the university; preparing journal entries and posting to the general ledger; gathering and consolidating the information required for the preparation of financial statements and other external financial reports; and preparing and reviewing the financial statements and other external reports. The Comptroller's Office is charged with the responsibility of preparing and issuing the annual financial statement; all departments are responsible for ensuring their fiscal information is accurate and processed/submitted timely.

In management's selection of procedures and techniques of control, the degree of control implemented is a matter of reasonable business judgment. The common guideline that should be used in determining the degree of internal controls implementation is that the cost of a control should not exceed the benefit derived.

The internal control guidelines for the Financial Reporting Cycle have been divided into three parts:

### **5.1 Accumulation of Financial Information**

### **5.2 Processing and Reporting of Financial Information**

### **5.3 Related Party Accounts**

## **5.1 ACCUMULATION OF FINANCIAL INFORMATION**

	<b><u>Standard of Internal Control</u></b>		<b><u>Risk if Standard is Not Achieved</u></b>
5.1.1	Accounting policies and procedures should be in accordance with GAAP and university policy. <i>Refer to risks: A-1, A-2, A-3, A-4</i>	A-1	The financial statements issued to the public may not be prepared in accordance with GAAP.
5.1.2	New accounting policies or changes to existing policies should be properly researched, reviewed and documented. Comptroller's Office/ ABOR should authorize all changes in accounting policies. <i>Refer to risks: A-1, A-2, A-3, A-4</i>	A-2	Reports may not be accurate and critical decisions may be based upon erroneous information.
5.1.3	All journal entries should be documented, reviewed and approved by appropriate level of personnel. <i>Refer to risks: A-1, A-2, A-4, A-5</i>	A-3	Policies and procedures may not be properly or consistently applied by or between departments.
5.1.4	Standardized journal entries should be utilized whenever possible. A process should be in place to identify standardized journal entries which were omitted or duplicated. <i>Refer to risk: A-5</i>	A-4	Governmental reporting requirements and/or loan restrictions may be violated.

- |       |  |     |  |
|-------|--|-----|--|
| 5.1.5 | Policies should be established to review and approve the accounting treatment of non-standard or unusual transactions.<br><i>Refer to risks: A-1, A-2, A-4, A-5</i>  | A-5 | Journal entries may be incorrectly prepared, duplicated, omitted or made for the purposes of misstating account balances to conceal irregularities or shortages. |
| 5.1.6 | Journal entries should be input to the general ledger in an accurate and timely manner. A process should be in place to ensure duplicate postings to the general ledger cannot occur.<br><i>Refer to risks: A-1, A-2, A-4, A-5</i> | A-6 | Accountability over recorded transactions may not be maintained.   |
| 5.1.7 | Contra-asset accounts should be utilized where necessary to maintain both proper asset valuation and detailed accounting records (e.g., receivables, inventory, and property).<br><i>Refer to risks: A-1, A-2, A-4, A-6</i>        |     |  |
| 5.1.8 | At least quarterly, an accrual should be made of all known liabilities which have not been processed for payment or recorded in the accounting records, as determined by university policy.<br><i>Refer to risks: A-1, A-4</i>     |     |  |
| 5.1.9 | All asset accounts should be reviewed at least annually to ensure values do not exceed net realizable value.<br><i>Refer to risks: A-1, A-4</i>  |     |  |

## **5.2 PROCESSING AND REPORTING OF FINANCIAL INFORMATION**

- | <b><u>Standard of Internal Control</u></b> |  | <b><u>Risk if Standard is Not Achieved</u></b> |  |
|--|--|--|--|
| 5.2.1                                      | Controls should be established to ensure all journal entries have been processed.<br><i>Refer to risks: B-1, B-2, B-5</i>  | B-1  | The financial statements issued to the public may not be prepared in accordance with GAAP applied on a consistent basis.                   |
| 5.2.2                                      | Adherence to monthly, quarterly and annual closing and reporting schedules and cutoffs should be strict and consistent.<br><i>Refer to risks: B-1, B-2, B-3, B-5</i>   | B-2  | Reports may not be accurate and critical decisions may then be based upon erroneous information.   |
| 5.2.3                                      | General ledger balances should be reconciled to the subsidiary ledgers or other supporting records on a timely basis; any differences should be promptly resolved and recorded.<br><i>Refer to risks: B-1, B-2, B-4, B-5</i> | B-3  | Financial statements may be misstated as journal entries may be omitted, recorded in the wrong period, duplicated and/or incorrectly made. |

5.2.4	<p>Clearing and suspense account transactions, including the transfer of expense, income or capital, should be resolved on a timely basis. Proper recognition of income or expense for these accounts should be made on at least a quarterly basis.</p> <p><i>Refer to risks: B-1, B-2, B-4, B-5</i></p>	B-4	<p>Errors and omissions in physical safeguarding, authorization and transaction processing may go undetected and uncorrected. Financial statements and records may be prepared inaccurately or untimely.</p>
5.2.5	<p>Consolidation, reclassification, and other adjustments of general ledger balances into financial statement formats should be adequately explained and documented to support the financial statements. Such adjustments should be approved by the Comptroller's Office.</p> <p><i>Refer to risks: B-1, B-2, B-3, B-4, B-5</i></p>	B-5	<p>Governmental reporting requirements and/or loan restrictions may be violated. Exposure to litigation increases substantially due to improper financial reporting.</p>
5.2.6	<p>Procedures and responsibilities should be established and maintained to ensure timely and accurate preparation, review, and approval of external financial reports including reports to governmental and regulatory bodies. These procedures should also ensure that such reports comply with the established requirements for financial information and related disclosures.</p> <p><i>Refer to risks: B-1, B-2, B-5, B-8, B-9</i></p>	B-6	<p>Confidential and proprietary information may be reviewed and disclosed by unauthorized individuals. The university's financial position and reputation may be adversely affected.</p>
5.2.7	<p>Comparisons and explanations of actual financial information to budgeted or forecasted information should be routinely (at least quarterly) completed; all significant variances should be researched.</p> <p><i>Refer to risks: B-1, B-2, B-4, B-5</i></p>	B-7	<p>Records may be destroyed or altered. This may result in the inability to prepare accurate and reliable financial statements.</p>
5.2.8	<p>Access to accounting and finance records and documents should be safeguarded.</p> <p><i>Refer to risks: B-6, B-7, B-8</i></p>	B-8	<p>Financial information required for budgeting, forecasting, or analysis may not be available.</p>
5.2.9	<p>Accounting and financial records should be retained in accordance with established record retention and tax requirements.</p> <p><i>Refer to risks: B-7, B-8, B-11</i></p>	B-9	<p>Policies and procedures may not be properly or consistently applied by or between departments. Financial statements may be prepared inaccurately or untimely.</p>
5.2.10	<p>Specific individuals should be given the responsibility to discuss financial results with individuals outside of the university.</p>	B-10	<p>The risk of error in the accumulation and reporting of financial information is increased.</p>

*Refer to risk: B-6*

- 5.2.11 All departments should comply with the current financial reporting requirements established by the Comptroller's Office. **B-11** The university may be exposed to litigation due to inadequate record maintenance.  
*Refer to risks: B-1, B-2, B-5, B-10*
- 5.2.12 Adherence to all legal reporting requirements (e.g., tax returns, statutory audits, etc.) should be strict and consistent.  
*Refer to risks: B-1, B-5*

### **5.3 RELATED PARTY ACCOUNTS**

Related party accounts pertain to transactions between the other approved financially-related organizations and the university.

- |       | <b><u>Standard of Internal Control</u></b>  |            | <b><u>Risk if Standard is Not Achieved</u></b>                              |
|-------|---|------------|---|
| 5.3.1 | All related party transactions should be recorded in accordance with university policy.<br><i>Refer to risks: C-1, C-2, C-3, C-4, C-5</i>   | <b>C-1</b> | Cash flows may not be maximized as projected receipts may not be accurate.  |
| 5.3.2 | All related party receivables/payables should be paid at "normal trade terms".<br><i>Refer to risks: C-1, C-2, C-3, C-4, C-5</i>  | <b>C-2</b> | Disputed transactions may not be identified and resolved on a timely basis. |
| 5.3.3 | At least quarterly, all locations should prepare an aging of related party account balances. Outstanding items should be resolved on a timely basis.<br><i>Refer to risks: C-1, C-2</i>   | <b>C-3</b> | The financial records and financial statements may be misstated.            |
| 5.3.4 | All related party loans between the university and other approved financially-related organizations are to be made only with the approval of and/or direction of ABOR and should be appropriately documented.<br><i>Refer to risks: C-1, C-4, C-5</i> | <b>C-4</b> | Transactions may not meet the overall goals of the university.              |
|       |   | <b>C-5</b> | Transactions may result in undesirable legal and/or tax implications.       |

## 6.0 COMPUTER SYSTEMS CONTROLS

Computer systems controls are an integral part of our internal control structure and are organized into two categories: General Computer System Controls and Application System Controls. Application systems are composed of programs written for or by the user to support the user's business functions. The responsibility for implementing and enforcing data processing controls resides with the system owners, users, and data processing equipment custodians. These standards apply universally to all computing environments, which include PC's, workstations, computer centers, and local area, facility and wide area networks.

In management's selection of procedures and techniques of control, the degree of control implemented is a matter of reasonable business judgment. The common guideline that should be used in determining the degree of internal controls implementation is that the cost of a control should not exceed the benefit derived. The specific processes included in the Computer Systems Controls Cycle are:

[6.1 System Owners and Custodians of Equipment](#)

[6.2 Physical Security and Environmental Controls](#)

[6.3 Computer Access Security](#)

[6.4 Network Security](#)

[6.5 Systems Development Methodology](#)

[6.6 Configuration Management](#)

[6.7 Computer Operations and Back up](#)

[6.8 Disaster Recovery Planning](#)

[6.9 Input Controls](#)

[6.10 Processing Controls](#)

[6.11 Output Controls](#)

[6.12 Paperless Transaction Processing](#)

### 6.1 SYSTEM OWNERS AND CUSTODIANS OF EQUIPMENT

Data processing users act as owners of application systems, data files, and programs. They are responsible for implementing and enforcing data processing controls and authorize access and change requests. For computer centers, IT personnel are the custodians of data processing equipment. For personal computers, workstations, computer integrated systems or local area networks, the custodian may be a business user or department management. Custodians are responsible for the operation and maintenance of data processing equipment.

	<b><u>Standard Of Internal Control</u></b>		<b><u>Risk If Standard Is Not Achieved</u></b>
6.1.1	Departments are responsible for ensuring an owner is assigned for each application system. System owners are the primary system users. For a system shared among multiple departments or business groups, the system owner is defined as the user or group of users with the primary responsibility for updating the application files. <i>Refer to risk: A-1</i>	A-1	Systems may not be properly maintained and controlled without system owner sponsorship.

- |       |  |     |  |
|-------|--|-----|--|
| 6.1.2 | <p>Department managers, in coordination with IT management, should maintain up-to-date lists of system owners.</p> <p><i>Refer to risks: A-3, A-4</i></p>  | A-2 | <p>Data processing controls may not be operating efficiently or effectively, system inherent and/or configurable controls may not be utilized, and/or access to the system may not be properly approved.</p> |
| 6.1.3 | <p>The system owner is responsible for implementing and enforcing data processing controls, approval of system requirements/design or security changes, assigning security classifications, authorizing access to the system data files, and acknowledging new system changes.</p> <p><i>Refer to risk: A-2</i></p>  | A-3 | <p>IT personnel may seek approval for system changes from someone other than the system owner.</p>   |
| 6.1.4 | <p>Department managers are responsible for ensuring a custodian is assigned for all data processing equipment including computer centers, remote processing sites, local area networks, engineering workstations, departmental and personal computers, and data storage sites.</p> <p><i>Refer to risk: A-5</i></p>  | A-4 | <p>Management personnel may change responsibilities without transferring system ownership.</p>   |
| 6.1.5 | <p>Custodians of data processing equipment and application data should:</p> <ul style="list-style-type: none"> <li>a. Provide a physical environment with safeguards against unauthorized removal or destruction of data or data processing equipment;</li> <li>b. Arrange for the backup and retention of critical application data files and programs in secure locations outside the facility where normal processing occurs;</li> <li>c. Arrange for equipment and/or alternate computing facilities sufficient to meet established disaster recovery priorities;</li> <li>d. Provide sufficient computer resources to respond to the data processing needs of the users who operate systems at their facility, department or local area network;</li> <li>e. Ensure procedures exist to comply with software licensing.</li> </ul> <p><i>Refer to risks: A-6 through A-10</i></p> | A-5 | <p>The responsibilities associated with operating and/or maintaining data processing facilities may not be clearly defined.</p>  |

6.1.6 Departments responsible for software development or maintenance are responsible for preparing and maintaining detailed data processing policies and procedures. The policies and procedures should include:

- a. Identification and operation of inherent, configurable and manual data processing controls and self-assessment processes.
- b. Criteria for management approval of inherent, configurable and manual data processing controls and system changes to move software from a test to production status:
- c. Documentation standards for system inherent, configurable, and manual controls, system architecture, logical design, and physical design; and
- d. Software coding standards that define program structure, guidelines for logic complexity, and data element naming conventions.

*Refer to risk: A-11*

Computer equipment may be damaged by fire or other natural causes or intentionally damaged by unauthorized persons.

- A-7 Backup files may not be available for processing in the event of a disaster.
- A-8 Our ability to conduct business may be significantly impaired in the event of a disaster at a computer or network site.
- A-9 Adequate computer resources may not be available to meet business requirements and growth.
- A-10 We may be liable for misuse or unauthorized copying of proprietary software.
- A-11 System inherent and/or configurable data processing controls may not be utilized and/or operating efficiently or effectively. Responsibilities associated with operating and/or maintaining system software operations and application documentation may not be clearly defined.



## GENERAL DATA PROCESSING CONTROLS

General data processing controls are primarily concerned with the operation and protection of computer resources, and the development and integrity of application systems and data. General data processing controls are the joint responsibility of user and data processing equipment custodians. The adequacy of general data processing controls within an organization provides the basis for the level of reliance placed upon application controls and, in turn, business and accounting controls for the accuracy and integrity of business and financial information.

## 6.2 PHYSICAL SECURITY AND ENVIRONMENTAL CONTROLS

	<u>Standard Of Internal Control</u>	<u>Risk If Standard Is Not Achieved</u>
6.2.1	<p>Department management may designate certain computing areas as requiring restricted access. Access to restricted computing areas should be limited to authorized individuals. Examples of restricted areas are computer centers and network file server locations. The following control techniques should be employed for these areas:</p> <p>a. Physical access to computer and network hardware, software, data, and documentation should be specifically authorized by management and restricted to only those personnel requiring such access for performance of assigned functional responsibilities; <i>Refer to risks: B-1, B-2</i></p> <p>b. All entrances/exits to restricted computing areas should be physically secured; <i>Refer to risks: B-1, B-2, B-3</i></p> <p>c. All keys, keycards, badges, etc., used to limit access to restricted computing areas should be confiscated by management upon employee termination or transfer. All combinations or passwords to restrictive areas and support areas should be changed periodically and upon employee termination or transfer; <i>Refer to risks: B-1, B-2, B-3</i></p>	<p>B-1 Computer hardware, software, data, and documentation may not be adequately protected from damage or theft.</p>

d. All physical access to computer hardware, software, data, and documentation by suppliers and visitors should be specifically authorized by management. All suppliers and visitors should be accompanied by authorized personnel; and  
*Refer to risks: B-1, B-2*

e. All removal of computer equipment and data files containing proprietary information should be specifically authorized by management, recorded, and reconciled. All data files removed should be handled in accordance with their contents.  
*Refer to risks: B-1, B-2*

- |       |   |     |  |
|-------|---|-----|--|
| 6.2.2 | Physical computer sites should be prepared and maintained in accordance with the environmental requirements specified by the supplier for the equipment.<br><i>Refer to risks: B-4, B-5, B-6, B-7</i>                         | B-2 | Unauthorized use, disclosure, modification, or destruction of systems and data could occur.  |
| 6.2.3 | Periodic inventories of computer hardware, data storage media, and supplies should be performed and reconciled.<br><i>Refer to risks: B-1, B-2, B-5</i>   | B-3 | Computer hardware may be used by unauthorized personnel to bypass normal security and operating controls and gain access to confidential systems and data.     |
| 6.2.4 | Main computer consoles and system management terminals should be accessible to only authorized operations personnel and all console activity should be recorded.<br><i>Refer to risks: B-2, B-3</i>                           | B-4 | Personnel may be subjected to unnecessary physical risk if environmental controls are not adequate.  |
| 6.2.5 | Computer and network hardware should not be located in unsecured, high traffic areas.<br><i>Refer to risks: B-1, B-2</i>  | B-5 | Loss of critical data could occur due to improperly installed, maintained, or stored computer hardware and storage media.                                      |
| 6.2.6 | Fire detection, prevention, and extinguishing systems and equipment should be installed at computer hardware sites, accessible to operations personnel, and periodically tested.<br><i>Refer to risks: B-1, B-4, B-5, B-7</i> | B-6 | Operational efficiency and reliability may be impaired and significantly disrupt processing.   |
| 6.2.7 | All computer hardware should be protected against electrical surges, water damage, and natural disasters with the potential to disrupt operations.<br><i>Refer to risks: B-1, B-4, B-5, B-7</i>                               | B-7 | Significant damage or destruction to computer hardware, software, and data could occur as a result of inadequate environmental monitoring and control systems. |

- 6.2.8 Computer hardware sites should not be constructed or located near any combustible or hazardous areas.  
*Refer to risks: B-1, B-4, B-5, B-7*
- 6.2.9 Computer hardware sites should be kept clean and free from combustible materials.  
*Refer to risks: B-1, B-4, B-5, B-7*
- 6.2.10 All computer hardware and software problems/errors should be recorded, monitored, and analyzed to ensure timely identification and correction.  
*Refer to risk: B-6*

### **6.3 COMPUTER ACCESS SECURITY**

The objectives of computer access security controls include protecting the integrity and accuracy of computer data/programs and providing for the security and privacy of confidential/proprietary information or sensitive data/programs.

	<b><u>Standard Of Internal Control</u></b>		<b><u>Risk If Standard Is Not Achieved</u></b>
6.3.1	<p>IT should ensure access security software is installed on all university equipment. The access security software may be part of the computer operating system. At a minimum, access security software should perform the following functions:</p> <p>a. Protect data files and programs from unauthorized access and/or alteration, theft, or destruction; <i>Refer to risks: C-1, C-2, C-3, C-4, C-8</i></p> <p>b. Include access control facilities that provide a means to segregate incompatible business functions through the use of unique user ID/password verification; <i>Refer to risks: C-1, C-2, C-3, C-4, C-5, C-10</i></p>	C-1	<p>University information may be disclosed or lost, which may adversely affect the university's financial position or reputation.</p>

c. Automatically require passwords be established and changed in accordance to and within the time periods established by policy. Passwords should be encrypted when stored and only decrypted during actual password validation processing; and  
*Refer to risks: C-1, C-2, C-3, C-4, C-8, C-9, C-11*

d. Have the ability to automatically create audit trail transactions showing significant security events such as unauthorized access to application data files/programs and unauthorized access attempts to applications/transactions that are proprietary and subject to fraud.  
*Refer to risks: C-1, C-2, C-3, C-4, C-8, C-9*

6.3.2 Custodians of computer equipment, in coordination with general and department managers, should appoint security administrators. The security administrator's function should be segregated from computer operations and systems development when practical.  
*Refer to risks: C-6, C-7*

C-2

Computers that process university data may not have adequate access security software.

6.3.3 IT, in coordination with general and department managers, should prepare and enforce security administration procedures. These procedures include:

C-3

Computer access security software or operating systems may not provide adequate minimum protective or detective security controls.

a. Establishing each new user account with documented management approval;

b. Granting access to production data files and programs;

c. Controlling the use of software procedures (privileges) that bypass normal access security controls; and

d. Defining, reporting, and investigating unauthorized access attempts in compliance with university policies.

*Refer to risks: C-7, C-8, C-9, C-12*

- 6.3.4 Security administrators, in coordination with departments, should establish procedures to maintain or deactivate employee computer accounts upon the employee's transfer or termination on a timely basis. Procedures should also be in place to detect active computer accounts assigned to terminated employees.  
*Refer to risks: C-13, C-14*
- C-4 Passwords to user computer accounts may be disclosed and allow unauthorized access to data and programs.
- 6.3.5 Application system owners should:
- a. Authorize access to the application and its data to appropriate users. Access should always be restricted on a "need to know" basis;  
*Refer to risks: C-10, C-15*
- b. Classify data files and programs consistent with policy on protecting appropriate information. The final decision as to classification rests with General Counsel;  
*Refer to risks: C-1, C-11, C-15, C-16*
- c. Label computer-generated reports and on-line video screens containing confidential or sensitive information with the proper classification; and  
*Refer to risks: C-1, C-11, C-16*
- d. Confirm annually with user department management the continued need for user's access. The confirmation process should be conducted with the assistance of the computer equipment's custodian and security administrator.  
*Refer to risk: C-17*
- C-5 Inadequate segregation of duties may result from the combination of system accesses and manual duties.
- 6.3.6 Department managers should ensure access granted to multiple systems does not compromise segregation of duties.  
*Refer to risks: C-10, C-17*
- C-6 Computer access security controls may not be implemented.
- 6.3.7 Management and IT Directors should approve the implementation of electronic data transfer systems, such as invoices, orders, or payments between the university and suppliers, customers, or contract services.  
*Refer to risks: C-1, C-18*
- C-7 Security administrators may have conflicting duties that would allow them to both change access security and system processing.

- 6.3.8 Computer systems or programs are considered in production status if systems/programs are relied upon by management for conducting, recording or reporting business operations. Software for production systems may be developed by IT departments, end users or vendors. Production systems may operate on mainframe, departmental, personal computers or wide-area/local-area networks. The following controls should exist to protect production computer software and data files: C-8
- Access to university data files and programs may be granted without proper authorization.
- a. Application programmers should not be provided with permanent update access to production software or data files. Management should grant specific authorization to programmers to change production software or data files to correct system failures; and
- b. Update access to production software or data files that are classified as confidential or proprietary to computer operations personnel or programmers who maintain or execute computer operating systems and/or system management software. Management should designate an appropriate individual to maintain records evidencing timely review of these logs.
- Refer to risks: C-1, C-11, C-15, C-16*
- 6.3.9 Suppliers, contract programmers and other non-university users should sign non-disclosure agreements before they are given direct access to our computer systems. Outside users who use our computer systems should have separate and unique computer accounts or user IDs. C-9
- Unauthorized access attempts may be made on a regular basis without detection.
- Refer to risks: C-1, C-11, C-15, C-16*

- 6.3.10 Custodians of computer equipment should ensure virus detection software is installed on the equipment when it is used for any university purpose.  
*Refer to risk: C-19*
- C-10 Access to multiple systems by the same user could result in an improper segregation of functions.
  - C-11 Sensitive information may be accessed and/or disclosed to unauthorized personnel.
  - C-12 Special access privileges may be granted which result in unnecessary or unauthorized access to university data files.
  - C-13 Terminated/transferred employees may gain access to and/or damage sensitive data, disrupt normal business processing, or disclose sensitive information to outsiders.
  - C-14 System access by terminated/transferred employees or accounts assigned to terminated/transferred employees may not be detected.
  - C-15 System users may be given access to data files and programs that are not required for their job functions.
  - C-16 Proprietary information stored on computer systems may not be properly protected.
  - C-17 Users may change job responsibilities but not change their system access requirements.
  - C-18 Business data may be transmitted without proper data processing or accounting controls resulting in erroneous orders, payments, or purchases.
  - C-19 Systems may become dysfunctional, resulting in business interruption, or critical data could be destroyed.

## **6.4 NETWORK SECURITY**

The objectives of network security controls include protection from unauthorized entry, misuse or alteration of information, and denial of service.

	<b><u>Standard Of Internal Control</u></b>		<b><u>Risk If Standard Is Not Achieved</u></b>
6.4.1	Custodians of data processing equipment who operate communications networks should document and maintain descriptions of their network topology. <i>Refer to risk: D-1</i>	D-1	Proprietary or confidential information may be disclosed or lost, which may adversely affect the university's financial position or reputation.
6.4.2	Standards based protocols should be used whenever they are available. Only tested and approved protocols will be allowed on our networks. <i>Refer to risks: D-2, D-3</i>	D-2	Data may not be accurately or completely transferred.
6.4.3	Network managers should utilize configuration, performance, fault, accounting, and security management tools to monitor networks. <i>Refer to risks: D-1, D-2, D-3, D-4, D-6, D-7</i>	D-3	Transmissions may not have adequate error correction.
6.4.4	Network addresses and names should be obtained and maintained as specified in IT standards. <i>Refer to risks: D-2, D-3, D-7</i>	D-4	Sensitive information may be accessed and/or disclosed to unauthorized personnel.
6.4.5	Custodians of computer equipment should make data encryption facilities available to protect data transmission of proprietary information. Passwords should be encrypted during network transmission. <i>Refer to risks: D-1, D-4, D-5</i>	D-5	Proprietary information stored on computer systems may not be properly protected.
6.4.6	Internal access to university networks should be controlled by single factor authentication (e.g., a unique user ID and password or token authentication). <i>Refer to risks: D-1, D-4, D-5</i>	D-6	Proprietary data may be disclosed to unauthorized personnel during transmission.
		D-7	Data bases may not contain accurate and complete information after system failure.



## 6.5 SYSTEMS DEVELOPMENT METHODOLOGY

<u>Standard Of Internal Control</u>		<u>Risk If Standard Is Not Achieved</u>
6.5.1	Departments responsible for software development and maintenance should define and document standard methodologies that should be used in developing and maintaining application systems. <i>Refer to risks: E-1, E-2, E-3, E-4</i>	E-1 Systems may be implemented which do not meet user requirements or comply with university software quality standards.
6.5.2	System development methodologies should include the following components:  a. Systems development projects should be segmented into measurable parts or phases with predefined deliverables and include the identification and documentation of system inherent, configurable and manual data processing controls; <i>Refer to risks: E-1, E-3</i>  b. Project team roles and responsibilities should be clearly defined and documented; <i>Refer to risks: E-2, E-4</i>  c. The system development project team, consisting of user, IT, and application owner personnel, should approve the completion of each major phase of development and controls documentation prior to progression to subsequent phases; and <i>Refer to risks: E-3, E-4, E-5, E-6</i>  d. Formal plans should be prepared for system development projects. Development and project plans should comply with university policies and procedures and include the following minimum attributes:  - A clear and accurate statement of business purpose and requirements for the proposed system; <i>Refer to risks: E-2, E-5, E-6</i>  - A feasibility study identifying possible software solutions and cost/benefit analysis; <i>Refer to risk: E-5</i>	E-2 Roles and responsibilities may be unclear, resulting in increased development cycle times or system inadequacies.  E-3 Systems may be implemented without approval of the system design, proper testing, or conversion resulting in erroneous processing.  E-4 Users may not actively participate in the development process, which could result in incorrect decisions during the design and testing phases.  E-5 Improper selection of data processing solutions to business problems may result from incomplete evaluation of alternatives.  E-6 The system design may not be properly documented and communicated resulting in uncontrolled or erroneous processing.

<p>- A detailed logical and physical system design; <i>Refer to risk: E-6</i></p>	E-7	<p>Individual programs and the entire system may not be adequately tested or may not operate as intended resulting in erroneous processing.</p>
<p>- System and user acceptance testing that will adequately test each system function and condition defined by the detailed logical and physical design; <i>Refer to risks: E-7, E-8</i></p>	E-8	<p>Users may not participate in acceptance of the system. The system may not operate properly and may not meet their needs.</p>
<p>- Specifications for conversion to the proposed system that will ensure the integrity of processing procedures, data processing controls, and data integrity; <i>Refer to risk: E-9</i></p>	E-9	<p>Data files may not be properly converted to the new system.</p>
<p>- Preparation of user procedures that document how users interact with the system and how that interaction is controlled. User procedures should reasonably answer questions on system operation, error correction, and data processing control; <i>Refer to risks: E-10, E-11</i></p>	E-10	<p>Users may not be able to recover from processing errors.</p>
<p>- Preparation of operations documentation that details how to operate the application system. The documentation should include procedures for restarting the application in the event of hardware or software failure; and <i>Refer to risks: E-12, E-13</i></p>	E-11	<p>Users may not be able to process independently of IT or other personnel who developed the system.</p>
<p>- Preparation of data processing controls documentation that details the new systems inherent and configurable controls in addition to the manual compensating controls surrounding the new system; and <i>Refer to risks: E-6, E-7</i></p>	E-12	<p>Operations personnel may not be able to operate the system.</p>
<p>- Training to sufficiently enable users to independently operate and control system processing. <i>Refer to risk: E-14</i></p>	E-13	<p>Operations and/or user personnel may not be able to recover from errors to continue business processing.</p>
	E-14	<p>Improperly trained users may not be able to adequately operate and control the system.</p>

## **6.6 CONFIGURATION MANAGEMENT**

Changes to the computing environment, including software, hardware, and operating procedures, should be authorized, documented, and tested.

	<b><u>Standard Of Internal Control</u></b>		<b><u>Risk If Standard Is Not Achieved</u></b>
6.6.1	Requests for changes to the production environment should include a business purpose or business impact analysis, and should be approved by the system owner. <i>Refer to risks: F-1, F-2</i>	F-1	Erroneous changes or changes resulting in improper use of the system may result from unauthorized system changes.
6.6.2	Changes to the production hardware and/or software environment should be tested. Tests should include sufficient conditions to ensure the new system configuration operates as intended. Testing should also include evidence that all requirements were tested to the satisfaction of the ultimate users of the system. <i>Refer to risks: F-3, F-4, F-5</i>	F-2	Programmers or other personnel preparing the system change may not adequately evaluate the impact of the change on business processing.
6.6.3	If the system change will result in the creation of journal entries or changes in journal entry account distribution, the change should be approved by the Comptroller's Office. <i>Refer to risks: F-5, F-6</i>	F-3	Changes may not be properly tested and their implementation may result in erroneous system processing.
6.6.4	Organizations or departments with responsibility for hardware or software should document and implement plans and procedures for Software Configuration Management. Software Configuration Management includes program change control, version and release management, status reporting, and changes to the operating system software. <i>Refer to risks: F-2, F-4</i>	F-4	Users and operations personnel may not be aware of system changes that could result in erroneous system processing.
6.6.5	Organizations or departments with responsibility for hardware or software should follow an approved, documented System Development Methodology when making maintenance changes to the production environment. <i>Refer to risks: F-4, F-7</i>	F-5	Financial or operational records may be misstated.

- |       |  |     |   |
|-------|--|-----|---|
| 6.6.6 | If distributed systems are designed with multiple copies of the same programs and data files on more than one computer, system-wide version controls should be developed to ensure proper versions of programs and data files are used throughout the system.<br><i>Refer to risks: F-1, F-3</i> | F-6 | Improper journal entries or account distribution may result from the system change. |
|       |  | F-7 | Users and operations personnel may not be able to recover from system failure.      |

## **6.7 COMPUTER OPERATIONS AND BACKUP**

Organizations or departments that operate computer equipment are responsible for ensuring that computers are operated in accordance with university policies and procedures.

<b><u>Standard Of Internal Control</u></b>	<b><u>Risk If Standard Is Not Achieved</u></b>		
6.7.1	Computer data files, programs, and system software should be backed up periodically to ensure continuity of business operations in the event of a hardware or software failure. <i>Refer to risks: G-1, G-2</i>	G-1	Programs and information assets could be lost due to hardware or software failure, or human error.
6.7.2	Each department is responsible for identifying data files that should be retained to comply with regulatory or statutory requirements, such as taxing authorities or government contracting agencies. <i>Refer to risks: G-3, G-4</i>	G-2	Tape files could be lost or erased in error.
6.7.3	Custodians of computer systems should maintain a system to record and track backup data files and other off-line media for recovery and retention purposes. <i>Refer to risk: G-5</i>	G-3	Business data files may not be properly retained and could subject the university to fines and penalties.
6.7.4	Backup information, including programs, data files, and supporting documentation, should be maintained at an off-site location not subject to the same peril as the normal computer processing site. <i>Refer to risks: G-6, G-7</i>	G-4	Data files retained for regulatory requirements may not contain complete and accurate data.
6.7.5	Personnel responsible for computer operations should prepare and maintain policies, procedures, and instructions on the operation of the computer and system software. <i>Refer to risk: G-8</i>	G-5	Backups may not be available and procedures may not be operating as management intended.

- G-6 In the event of a disaster, critical files may be destroyed that could prevent recovery of business processing.
- G-7 The ability to continue business operations in the event of an emergency may be impaired.
- G-8 Procedures for the operation and control of computer systems may not be properly communicated or performed.

## **6.8 DISASTER RECOVERY PLANNING**

The objective of disaster recovery planning is to ensure the continuity of university business operations in the event of unanticipated computer processing disruptions such as operational failures or site disasters that destroy or prevent access to the computer equipment, data, and software.

	<b><u>Standard Of Internal Control</u></b>		<b><u>Risk If Standard Is Not Achieved</u></b>
6.8.1	Custodians of computer applications, equipment and facilities, in coordination with application system owners, are responsible for arranging for alternative equipment and/or computing facilities. Alternative equipment or facilities should be adequate to recover critical on-line, batch processing & network systems.	H-1	The university may incur a severe disruption of business operations if computer equipment custodians are not able to recover in the event of an unanticipated processing disruption.

Disaster recovery plans should include the following:

a. A determination of the most effective alternative processing method for both critical and non-critical applications. Alternatives include:

- Processing at another university site;

- Processing at an alternative computer site using a reciprocal agreement with another university or a conditional site maintained by a recovery site vendor;

or

- Not processing applications until computer equipment and or sites are restored;

b. A plan detailing IT and user personnel requirements and special skills needed in the event of an unanticipated processing disruption; and

c. Storage of critical replacement forms, supplies, and documentation at off-site storage.

*Refer to risks: H-1, H-2, H-3, H-4*

- |       |  |     |   |
|-------|--|-----|---|
| 6.8.2 | <p>Application system owners should classify their application's recovery priority. This priority should be used by computer equipment custodians to determine the sequence of restarting critical application systems in the event of an unanticipated processing disruption. The priority assessment should include the following:</p> <ul style="list-style-type: none"> <li>a. Quantify the risk in terms of dollars or other measurable terms due to partial or total loss of processing the application;</li> <li>b. Assess the lead time between loss of application processing and adverse impact on university operations as part of determining acceptable down time; and</li> <li>c. Obtain agreement from department management on the classification as to critical or non-critical.</li> </ul> <p><i>Refer to risks: H-1, H-2, H-3</i></p> | H-2 | <p>Critical systems may not be recovered first.</p>   |
| 6.8.3 | <p>Detailed disaster recovery plans should be documented and tested periodically to ensure recovery can be accomplished. Where tests of the full disaster recovery plans are found to be impractical due to business conditions or the cost of testing, test plans should be developed and implemented to test portions of the plan.</p> <p><i>Refer to risks: H-1, H-4</i></p>  | H-3 | <p>The university could sustain substantial financial loss if critical computer systems and equipment were severely damaged or destroyed.</p> |
| 6.8.4 | <p>Custodians of computer systems, in conjunction with application owners, should review and update the disaster recovery plan annually. Updates should reflect changes in applications, hardware and/or software.</p> <p><i>Refer to risk: H-4</i></p>  | H-4 | <p>The disaster recovery plans may not be effective.</p>  |

## APPLICATION SYSTEM CONTROLS

Application system controls are concerned with the integrity, accuracy, and completeness of data input to, and processed, stored, and produced by, the application system.

### 6.9 INPUT CONTROLS

	<u>Standard Of Internal Control</u>		<u>Risk If Standard Is Not Achieved</u>
6.9.1	All manually input or interfaced transactions should be properly originated and authorized and include evidence of authorization prior to processing. <i>Refer to risks: I-1, I-2</i>	I-1	Unauthorized transactions may be processed.
6.9.2	Manually input or interfaced data should be subjected to sufficient edits and validations, including duplicate and completeness checks, to prevent or detect data input errors. <i>Refer to risks: I-1, I-2</i>	I-2	Invalid or erroneous data may be processed and affect operating and/or financial decisions.
6.9.3	Manually input or interfaced data rejected by application system edit and validation procedures should be controlled to ensure that input errors are identified and corrected, and data is re-input to the system on a timely basis. <i>Refer to risks: I-3, I-6</i>	I-3	Rejected input may not be corrected and re-input into the system resulting in incomplete processing.
6.9.4	Application systems should provide an audit trail from the input transactions recorded by the system to the source transaction and originating user or system. <i>Refer to risks: I-4, I-5</i>	I-4	An adequate audit trail may not exist to provide a means of substantiating input transactions.
		I-5	Financial and/or operating personnel may not be able to explain transaction activity or account balances.
		I-6	Untimely correction of rejected items may result in incorrect records and financial statements.





## 6.11 OUTPUT CONTROLS

	<u>Standard Of Internal Control</u>		<u>Risk If Standard Is Not Achieved</u>
6.11.1	Application systems should provide activity logs which evidence:  a. All input transaction data, including data received from other systems;  b. Additions or changes to master file or reference table data; and  c. Internally generated transactions. <i>Refer to risks: K-1, K-2, K-3</i>	K-1	Application systems may not produce adequate audit trail, input, or processing reports to control processing.
6.11.2	Application system audit trails should provide for unique identification of processed transactions to allow them to be traced and vouched through the system. <i>Refer to risks: K-1, K-2, K-3</i>	K-2	Erroneous or unauthorized changes to system data may not be detected.
6.11.3	All on-line video screens or reports should include sufficient information to ascertain their origin, period covered, contents, and completeness. <i>Refer to risks: K-1, K-2, K-3, K-4</i>	K-3	System audit trails may not be adequately generated or maintained.
6.11.4	Data processing custodians and application system users should establish and implement procedures to ensure that proprietary reports are promptly collected by authorized users, and that remote printers or report distribution sites are secured. <i>Refer to risk: K-4</i>	K-4	Proprietary or confidential information may be unintentionally disclosed to the detriment of the university.
6.11.5	Data files, data storage media, and computer reports (including carbons and fiche) containing proprietary information should be properly destroyed after their useful lives. <i>Refer to risk: K-4</i>		

## 6.12 PAPERLESS TRANSACTION PROCESSING

Paperless transaction processing or electronic data interchange (EDI) refers to a business operation in which electronically processed or stored information replaces the traditional paper trail of evidence. Paperless processing control provisions, like those for a manual processing environment, are concerned with the authorization, accuracy, and completeness of transactions. Thus, all relevant business cycle and application controls apply.

	<b><u>Standard Of Internal Control</u></b>		<b><u>Risk If Standard Is Not Achieved</u></b>
6.12.1	Paperless transactions should include evidence of proper authorization. Effective logical access and security administration control should be in place to ensure reliance upon electronic authorization. <i>Refer to risk: L-1</i>	L-1	Transactions may not be legitimate, introducing the risk of fraudulent processing and legal liabilities.
6.12.2	Controls should be in place to ensure the authenticity of the transaction source. The minimum authentication and security requirements should be defined by business areas and their customers. <i>Refer to risk: L-2</i>	L-2	Transaction authenticity or integrity may not be assured, decreasing the reliability of the information and also introducing the risk of fraudulent or erroneous processing.
6.12.3	The content of paperless transactions should not be altered through the transmission process, i.e. from point of origination to receipt. Each component in the paperless processing system, from manual entry and computer operations to application edits and system security, should encompass the controls necessary to ensure transaction integrity. In addition, there should be adequate audit trails at key points in the transmission path. <i>Refer to risk: L-2</i>	L-3	Paperless records may not be retained, or securely held, thus introducing risk of information loss and possible regulatory penalties.
6.12.4	Retention of paperless transactions should be managed to ensure that the electronic records are available, authentic, and reliable and reproducible. Retention should be in compliance with retention policies and schedules. <i>Refer to risk: L-3</i>	L-4	Responsibilities may be unclear, causing the university to be unnecessarily liable for system failure or transaction loss.

6.12.5 For EDI-based processes, Trading Partner Agreements (TPA's) should be prepared and approved by the legal department prior to the initiation of EDI processing. TPA's should identify the specifications for transaction processing as well as trading partner responsibilities, terms and conditions, and corresponding liabilities.

*Refer to risk: L-4*

6.12.6 Where Value-Added Networks (VAN's) are utilized, operational, security and legal liabilities for the integrity of university information should be contractually defined.

*Refer to risk: L-4*

## **7.0 ENVIRONMENT, HEALTH and SAFETY (EHS)**

The EHS Cycle includes an overview of those controls necessary for compliance with selected governmental requirements and guidance on where they may be applicable in the university environment.

It is the policy of the university to conduct all business activities in a responsible manner, free from recognized hazards; to respect the environment, health, and safety of our employees, customers, suppliers, partners and community neighbors; to foster the sustainable use of the earth's resources; and to comply with all applicable environmental, health, and safety laws and regulations of locations where we operate, while committing ourselves to continuous improvement in our EHS management systems and safety programs.

	<b><u>Standard of Internal Control</u></b>		<b><u>Risk if Standard is Not Achieved</u></b>
7.1	All facilities should have knowledge of, and, as applicable, written policies/procedures and other necessary controls to ensure compliance with all applicable EHS laws and regulations. <i>Refer to risks: A-1, A-2, A-3</i>	A-1	Government laws and regulations may be violated.
7.2	The university should conduct audits of EHS activities at its facilities. In addition, each department should ensure that annual EHS self audits are completed at each of their facilities. <i>Refer to risks: A-1, A-2, A-3</i>	A-2	Civil and criminal penalties against the university and/or individual employees may occur.
7.3	All university facilities and operations should meet applicable internal EHS policies, including but not limited to covering:  a. EHS Training b. Hazardous Materials Management; c. Emergency Preparedness and Response; d. Occupational Health; e. Injury and Illness; f. Personal Safety; g. Equipment Safety;	A-3	Critical decisions may be based on erroneous information.

*Refer to risks: A-1, A-2, A-3*

## **8.0 MISCELLANEOUS CYCLES**

In developing a system of general and administrative internal controls, several functions or requirements could not be precisely included in any other specific business cycle. The category "Miscellaneous Cycles" is a logical and appropriate vehicle to include specific control requirements for these important, yet somewhat general, control requirements. This section of the manual will be used for subsequent additions of specific procedures.

In management's selection of procedures and techniques of control, the degree of control implemented is a matter of reasonable business judgment. The common guideline that should be used in determining the degree of internal controls implementation is that the cost of a control shouldn't exceed the benefit derived.

### **8.1 Capital Assets**

#### **8.2 Subsequent Additions/Future Use**

## **8.1 CAPITAL ASSETS**

	<b><u>Standard of Internal Control</u></b>		<b><u>Risk if Standard is Not Achieved</u></b>
8.1.1	Detailed records of capital assets should be maintained and should include information regarding asset description, location, asset tag number, etc., where appropriate. <i>Refer to risks: A-1, A-2, A-4, A-5</i>	A-1	Substantiation of account balances and verification of the related assets may not be possible. Cost and accumulated depreciation information required for financial reporting and/or subsequent disposal may not be available.
8.1.2	Detailed capital asset records should be safeguarded. <i>Refer to risk: A-3</i>	A-2	Any errors or omissions in the physical safeguarding, authorization, or processing of transactions may not be detected.
8.1.3	Detailed capital asset records should be periodically reconciled to the general ledger and all differences researched and resolved. <i>Refer to risks: A-2, A-4, A-5</i>	A-3	Records may be lost, stolen, destroyed, or altered resulting in the inability to prepare financial records or the concealment of an asset misappropriation.
8.1.4	Procedures should be established to differentiate between capitalization or expensing of asset purchases. <i>Refer to risks: A-5, A-6</i>	A-4	Assets may be lost, stolen, destroyed, or temporarily diverted.
8.1.5	The depreciation method and useful life used for depreciating individual assets should be established in compliance with GAAP and ABOR guidelines. <i>Refer to risks: A-5, A-11</i>	A-5	The financial statements, records, and operating reports may be misstated, inconsistent, and/or not prepared in accordance with GAAP. Critical decisions may be based upon erroneous information.
8.1.6	Asset identification/bar-code tags should be promptly affixed to capital assets except where inappropriate (e.g., modular furniture, building partitions, etc.). <i>Refer to risks: A-4, A-7, A-8</i>	A-6	Acquisitions may be incorrectly capitalized or expensed.

8.1.7	Formal ABOR approval is required for certain asset acquisitions such as land, buildings, and computer systems. <i>Refer to risk: A-9</i>	A-7	Lost, scrapped, transferred, and/or sold assets may not be correctly identified, and the detailed records may not be properly updated.
8.1.8	Expenditures incurred in excess of approved capital addition levels require additional management approval. <i>Refer to risk: A-9</i>	A-8	Subsequent physical verification and reconciliation of fixed assets to detailed records may not be possible.
8.1.9	Verification of fixed assets should be completed at least annually and compared to detailed records and the general ledger. Any differences should be recorded in a timely manner. <i>Refer to risks: A-2, A-4, A-5</i>	A-9	Anticipated benefits of proposed equipment and facility acquisitions may not meet university criteria for making the investment. Funds may not be available to finance the asset acquisition.
8.1.10	All university assets should be safeguarded. <i>Refer to risk: A-4</i>	A-10	Assets may be sold or retired without authorization, may be unaccounted for, or may be sold at an unacceptable price, or may be used in other areas of the university.
8.1.11	Any significant accumulations of idle or surplus equipment should be reported to the Property Control department. <i>Refer to risks: A-4, A-5, A-10</i>	A-11	The useful life assigned or the depreciation method applied to a particular asset may be incorrect resulting in incorrect charges to operating results.
8.1.12	Any sale or disposal of university assets should be in accordance with policy. Sales will be made and recorded in the accounting records only after funds are deposited. Control procedures should be instituted to ensure all dispositions are accounted for properly. <i>Refer to risks: A-4, A-5, A-10, A-13</i>	A-12	Transactions may not have been recorded due to inadequate processing controls.
		A-13	If review procedures are inadequate, appropriate corrective actions may not be initiated on a timely basis.

## 9.0 LOSS PREVENTION CYCLE

The Loss Prevention Cycle includes the functions necessary for all members of management to effectively fulfill their ongoing responsibility to safeguard the university's physical assets against loss or compromise and to provide for the safety and security of employees, to maximize efficiency and enhance the maintenance of business continuity.

In management's selection procedures and techniques of control, the degree of control implemented is a matter of reasonable business judgment. The common guidelines that should be used in determining the degree of internal controls implementation is the cost of a control should not exceed the benefit derived.

The specific functions in the Loss Prevention Cycle are:

### 9.1 Physical Security

### 9.2 Access Controls

### 9.3 Personnel Security

### 9.4 Physical Asset Protection

### 9.5 Protection of Trademarks/Logos

## 9.1 PHYSICAL SECURITY

	<b><u>Standard of Internal Control</u></b>		<b><u>Risk if Standard is Not Achieved</u></b>
9.1.1	All university facilities should be designed to guard against forced and unauthorized entry, theft, property damage, and injury to personnel. <i>Refer to risks: A-1 through A-9</i>	A-1	Unauthorized persons may enter onto or into university property.
9.1.2	All university locations should display appropriate notice identifying the premises as university property. <i>Refer to risks: A-1, A-4, A-7</i>	A-2	Unauthorized or unlawful entry may be attempted or made into university premises without detection.
9.1.3	A member of the university police department should be part of the due diligence process (including site selection) for new construction and leased properties. <i>Refer to risks: A-1 through A-9</i>	A-3	University assets, such as supplies, property, materials and technology may be stolen, damaged or otherwise compromised.
9.1.4	Security systems will be tested at least semi-annually and records maintained. <i>Refer to risks: A-1, A-2, A-3, A-4, A-7</i>	A-4	Consistent application of security measures and procedures may not occur.
9.1.5	All university operations shall undergo a regularly scheduled physical and operational security review in accordance with policy. Records of reviews and corrective actions shall be maintained by the university. <i>Refer to risks: A-1 through A-9</i>	A-5	Records may be destroyed, stolen or altered by unauthorized individuals.



- A-6 Unauthorized access to and/or disclosure of confidential/proprietary information could adversely affect the university's financial position and reputation.
- A-7 Security for students, employees and visitors may be inadequate.
- A-8 Internal controls may be circumvented or may not be executed.
- A-9 Disruption to operations, as a result of high crime, violence and social-economic instability.

## 9.2 ACCESS CONTROLS

	<b><u>Standard of Internal Control</u></b>		<b><u>Risk if Standard is Not Achieved</u></b>
9.2.1	Identification card should be carried by all employees and students at all times while on university property. <i>Refer to risks: B-1, B-2, B-4, B-6</i>	B-1	Unauthorized persons may enter onto or into university property.
9.2.2	Facility management and/or university police should implement procedures based upon policy to govern the access and movement of non-employees on university property. <i>Refer to risks: B-1 through B-6</i>	B-2	University assets, such as supplies, property and technology, may be stolen, damaged or otherwise compromised.
9.2.3	All visitors should be escorted at all times while on university property <i>Refer to risks: B-1 through B-6</i>	B-3	Required documentation of non-employee access to university property will not be maintained.
9.2.4	All locations will give notice that the university reserves the right to inspect hand-carried items, including briefcases and handbags. Local management will determine inspection procedures. <i>Refer to risks: B-1, B-2, B-4, B-5, B-6</i>	B-4	Security for university students, employees and visitors may be inadequate.
9.2.5	Access should be restricted to areas with sensitive information and/or materials. <i>Refer to risks: B-1, B-2, B-4, B-5, B-6</i>	B-5	Internal controls may be circumvented or may not be executed.
		B-6	Unauthorized access to and/or disclosure of confidential/proprietary information could adversely affect the university's financial position and reputation.

## **9.3 PERSONNEL SECURITY**

	<b><u>Standard of Internal Control</u></b>		<b><u>Risk if Standard is Not Achieved</u></b>
9.3.1	All applicants should undergo a pre-employment screening process prior to being hired by the university. Levels of screening (higher or lower) may differ based upon sensitivity of designated positions. <i>Refer to risks: C-1 through C-7</i>	C-1	Individuals may be employed who falsified previous employment, educational or other relevant information and therefore do not meet our hiring criteria or standards.
9.3.2	All new employees should sign applicable compliance documents. <i>Refer to risks: C-2, C-3, C-4, C-5, C-6, C-7</i>	C-2	University assets, such as supplies, property, materials and technology may be stolen, damaged or otherwise compromised.
9.3.3	Department management should ensure that non-employees (i.e., contractors, consultants, vendors, suppliers) complete an approved Non-disclosure or Confidentiality Agreement prior to receiving university proprietary information. <i>Refer to risks: C-2, C-3, C-4, C-5, C-6, C-7</i>	C-3	Consistent application of security measures and procedures may not occur.
9.3.4	Department management will insure that all employees and contractors are aware of security policies and practices. <i>Refer to risks: C-2, C-3, C-4, C-5, C-6, C-7</i>	C-4	The university may suffer due to loss of proprietary information.
9.3.5	Department management will establish a process to insure that separated employee's and contractor's badges, key cards and other university property are collected, and access to systems are disabled. <i>Refer to risks: C-2, C-3, C-5, C-7</i>	C-5	Unauthorized access to and/or disclosure of confidential/proprietary information could adversely affect the university's financial position and reputation.
		C-6	Laws and government regulations may be violated resulting in fines, penalties, lawsuits or contingent liabilities.
		C-7	Unauthorized persons may enter onto or into university property.

## **9.4 PHYSICAL ASSET PROTECTION**

	<b><u>Standard of Internal Control</u></b>		<b><u>Risk if Standard is Not Achieved</u></b>
9.4.1	A property control process will be established to ensure proper accountability of physical assets and compensating controls are established at all locations. <i>Refer to risks: D-1, D-2, D-5, D-7</i>	D-1	University assets, such as supplies, property and technology may be stolen, damaged or otherwise compromised.
9.4.2	Managers and employees will report incidents of loss, theft, fraud, embezzlement, threats, suspicious activity and inventory shortages to the appropriate party. Incidents can also be reported anonymously to the Safety and Compliance Hotline. <i>Refer to risks: D-1 through D-8</i>	D-2	Consistent application of security measures and procedures may not occur.
9.4.3	Managers and employees will report code of conduct incidents, unlawful or unethical practices to the appropriate parties. <i>Refer to risks D-1 through D-8</i>	D-3	Records may be destroyed, stolen or altered by unauthorized persons.
9.4.4	University administration will document all reported incidents in a centralized database, and insure that the appropriate organizations are notified. <i>Refer to risks: D-2, D-5, D-6, D-7</i>	D-4	Unauthorized access to and/or disclosure of confidential/proprietary information could adversely affect the university's financial position and reputation.
9.4.5	Incidents relating to misuse of the university's computers and networks, including voice and data communications, should be reported to the appropriate parties. <i>Refer to risks: D-1 through D-8</i>	D-5	The university's ability to conduct business may be significantly impaired.
9.4.6	Sensitive, hazardous and/or high value assets or materials should be properly controlled and stored in a secured area or container. <i>Refer to risks: D-1 through D-7</i>	D-6	Security for university students, employees and visitors may be inadequate.
		D-7	Internal controls may be circumvented or may not be executed.
		D-8	Laws and government regulations may be violated resulting in fines, penalties, lawsuits or contingent liabilities.

## **9.5 PROTECTION OF TRADEMARKS/LOGOS**

	<b><u>Standard of Internal Control</u></b>		<b><u>Risk if Standard is Not Achieved</u></b>
9.5.1	Department management will be responsible for protecting university trademarks/logos, consistent with policy. <i>Refer to risks: E-1 through E-6</i>	E-1	University assets, such as property, material and technology may be stolen, damaged or otherwise compromised.
9.5.2	Department management will ensure that all employees are aware of their responsibility to safeguard university trademarks/logos. <i>Refer to risks: E-1 through E-</i>	E-2	Records may be destroyed, stolen or altered by unauthorized persons.
9.5.3	Use of university trademarks/logos should be monitored to preclude unauthorized use. <i>Refer to risks: E-1 through E-</i>	E-3	The university may suffer due to loss of its trademark/logo control.
9.5.4	University trademark/logo compliance audits should be conducted periodically based on risk, and resolved accordingly. <i>Refer to risks: E-1 through E-6</i>	E-4	Unauthorized use of the university's trademarks or logos could adversely affect its financial position and reputation.
9.5.5	All outsourcing and third party agreements should include Non-disclosure or confidentiality agreements to ensure the university's trademarks/logos are used only with express permission. <i>Refer to risks: E-1 through E-6</i>	E-5	Laws and government regulations may be violated resulting in fines, penalties, lawsuits or contingent liabilities.
		E-6	Consistent application of security measures and procedures may not occur.

## 10.0 INTELLECTUAL PROPERTY (IP)

The university's future is highly dependent on its technological competence. Technology is a real asset in the same sense that land, building and physical equipment are assets, except that these latter assets are much easier to acquire and replace. Technology such as patents, copyrights, trademarks, and research is represented primarily in the form of intangible assets, so it is very often difficult to define and protect compared with the visible, tangible properties such as plant and machinery. The objective of the IP section is to define: responsibilities of IP owners and custodians; controls over IP transfers, specific controls for patents, and copyrights ensuring university ownership; controls over research information; and controls mitigating the risk of infringing IP rights owned by others. For purposes of this document, IP includes copyrights, patents, and any other legal claims to ownership of university research or information.

### **Definition:**

*Intellectual Property (IP)* - legal rights owned by an individual or university in technology, information, products, processes, designs, and other intellectual work products. Patents, trademarks, and copyrights are the legal instruments designed to protect the university's rights.

	<b><u>Standard of Internal Control</u></b>		<b><u>Risk if Standard is Not Achieved</u></b>
10.1	The sale, purchase, application for or license of IP rights should be approved by the appropriate level of management. In addition, all IP transfers in and out of the university should take place under stipulated conditions defined by ABOR and university policy and procedures.	A-1	IP transfers may have negative impact on various university research and technologies, and preclude the university from meeting strategic goals.
	Appropriate approval is required for:		
	a. All transfers of IP rights in or out of the university, unless covered by an existing agreement;	A-2	Technology and/or IP developed by one department could be transferred outside of the university through another area, without the approval of the department that developed the IP.
	b. All agreements, in which the university funds research and does not own or fully own the results; and		
	c. All agreements, in which the university is contractually precluded from performing research in a specific area or using a specified product or partner. <i>Refer to risks A-1 through A-4</i>	A-3 A-4	One department may enter into an agreement precluding other departments from performing research and development without knowledge and approval of all departments.  Lack of timely documented approval may negatively impact operations where IP licensing plays a significant role.
10.2	Inventories of university-owned patents, registered trademarks, and copyrights should be performed at least on an annual basis. <i>Refer to risks: A-5 through A-8</i>	A-5	The university may lose IP rights through failure to meet regulatory requirements or changes in the law.

- 10.3 All licensing agreements should be reviewed by appropriate authorized personnel trained for, and having job duties including, modifying or negotiating contracts.  
*Refer to risk A-9*
- 10.4 All appropriate departments should provide an ongoing IP education and awareness program for appropriate personnel. The objective of the IP program is to encourage employees to create novel ideas, ensure university IP rights are adequately protected, and mitigate the risk of infringement of IP rights owned by others.  
*Refer to risk: A-10*
- A-6 The university may fail to enforce IP rights.
- A-7 The university may not fully utilize its IP in cross-licensing, joint ventures, joint research, etc.
- A-8 Critical decisions may be based on erroneous or incomplete information.
- A-9 Failure to comply with statutory requirements may result in financial exposure to the university.
- A-10 University IP rights may not be identified or they may be lost. The university may be exposed to a financial risk caused by an infringement of IP rights owned by others.