

**MINUTES**  
**JOINT MEETING**  
**FINANCE/AUDIT AND CONSTRUCTION COMMITTEE**  
**UNIVERSITY OF SOUTHERN INDIANA**  
**BOARD OF TRUSTEES**

**March 5, 2009**

The Finance/Audit and Construction Committees of the University of Southern Indiana Board of Trustees met in joint session on Thursday, March 5, 2009, in Carter Hall in the University Center. In attendance were Committee Chair Jeffrey L. Knight and Trustees John M. Dunn and Ronald D. Romain '73. Trustees Ira G. Boots and Amy MacDonell were absent. Others in attendance were Vice President for Business Affairs and Treasurer Mark Rozewski and Vice President for Government and University Relations Cynthia S. Brinker.

Committee Chair Jeff Knight called the meeting to order at 8:35 a.m.

Vice President Rozewski began the meeting by reviewing a change in the Finance/Audit Committee, a standing committee, and in the Construction Committee, an ad hoc committee. It has been the practice of University and the Trustees to consider these committees separately, even though they meet together and are comprised of the same membership. For purposes of record-keeping and meeting planning, the Construction Committee and its responsibilities will be subsumed into the Finance/Audit Committee following this meeting.

**1. APPROVAL OF CONSTRUCTION CHANGE ORDERS**

Mr. Knight called on Vice President Rozewski, who reviewed change orders to construction projects. He noted change orders in amounts up to \$25,000 may be issued by the Vice President for Business Affairs and change orders over \$25,000 require the Committee's approval. He referred the Trustees to Attachments A and B, summaries of construction change orders. Those in Attachment B require approval.

On a motion by Mr. Romain, seconded by Mr. Dunn, the following change orders detailed in Attachment B were approved.

**BUSINESS AND ENGINEERING CENTER PROJECT**

**SUPPORT SERVICES BUILDING**  
**Key Construction Company – Contractor**

CO 9	Install overhead garage door, card reader for opening, paved access drive, and associated work on the west side of the warehouse	\$34,452
CO 10	Install video camera and alarm system for security of art storage area	\$43,763

**2. APPROVAL OF CONSTRUCTION BIDS FOR THE UNIVERSITY CENTER EXPANSION PROJECT**

At its meeting on November 1, 2007, the Board of Trustees authorized the Construction Committee to review construction bids and award contracts or reject any and all bids for the construction of the University Center Expansion/Renovation project.

Construction bids for the University Center Expansion/Renovation project were received on February 17, 2009, and reviewed by the architects and University staff. An analysis of the bids in Attachment C is appended to the file copy of these minutes.

Mr. Knight called on Vice President Rozewski, who reported that the bids for the project were approximately five percent over the target of \$17,650,000, possibly because of changes in the market and possibly because it

is typically more difficult to renovate and adapt building that to build new structures. He referred to the summary of the bids received (Attachment C) and recommended an increase in the overall project budget from \$17,650,000 to \$18,400,000 and the award of the general contract in the amount of \$10,102,900 to Weddle Bros. Building Group, LLC. Vice President Rozewski also recommended awarding the mechanical contract for \$1,809,006 to Deig Brothers Lumber and Construction Co., Inc. and the electrical contract for \$2,586,298 to Capital Electric. The total amount of the awards recommended is \$14,498,204. Mr. Rozewski noted the total includes the base bid plus alternates 2, 3 and 5 for all the contractors and alternate 4 for the electrical contractor.

Mr. Rozewski noted construction will begin in April and the completion date is expected to be January 2011.

On a motion by Mr. Romain, seconded by Mr. Dunn, the staff recommendation regarding construction bids for the University Center Expansion/Renovation Project was approved.

### **3. REVIEW OF COMPLETED AUDITS AND APPROVAL OF THE ANNUAL AUDIT PLAN**

Mr. Knight called on Mr. Rozewski who introduced Diana Biggs, director of Internal Audit, for a report on internal controls, a summary of audits and activities conducted by the Internal Audit Department in 2007-2008 (Attachment D), and a review of the proposed 2009 Annual Audit Plan (Attachment E). Attachments D and E are appended to the file copy of these minutes.

Ms. Biggs referred the Trustees to reports in Attachment D (Pages 5-13) of internal controls. These include Accounting Controls, Information System Controls and Administrative Controls. She shared examples of deviations from best practices that do not have compensating controls in place and how these will be addressed by the department staff.

Ms. Biggs reviewed a summary audits completed in calendar year 2008 (pages 14-16). She highlighted audits related to Time Worked verses Time Reported, security access to the USI Banner enterprise management system, and federal grant compliance.

She reviewed the scheduled audits for calendar year 2009 (Attachment E). On a motion by Mr. Dunn, seconded by Mr. Romain, the Annual Audit Plan for Calendar Year 2009 (Attachment E) was approved.

Mr. Romain requested a regular audit update and asked for details about any deviation to the annual report. He asked if the Audit Department was an adequate size and what Ms. Biggs considered its limitations.

Mr. Knight reported the outcome of the audit report satisfies the University's responsibility for establishing, maintaining, and assessing internal controls. He commended the University staff for its work.

There being no further business, the meeting adjourned at 9:30 a.m.

## ATTACHMENT A

### Summary of Construction Change Orders Authorized by the Vice President for Business Affairs

#### 1. RECREATION AND FITNESS CENTER EXPANSION PROJECT

##### Arc Construction Company – General Construction Contractor

CO G-3	Add gypsum board recess for television in Quiet Lounge per PR G-15	
	Delete painting of structural steel per PR G-12	
	Use alternate coating in washer discharge trench per PR G-14	\$ 608

#### 2. BUSINESS AND ENGINEERING CENTER PROJECT

##### **BUSINESS AND ENGINEERING CENTER** Weddle Brothers Building Group LLC – General Contractor

CO 1	Several changes to the project, including credit for using galvanized (in lieu of stainless steel) relief clips and to delete one layer of insulation on roof, add one project site sign, add foundation drain piping, and other minor changes to project details	(\$45,595.16)
------	---	---------------

##### **SUPPORT SERVICES BUILDING** Key Construction Company – Contractor

CO 5	Reroute refrigerant piping in Room 201 and raise dust collector duct in Room 128	\$ 3,456
CO 6	Remove unsuitable soils under roadway, install wood blocking in walls, add carpet in office area, rework entrance road and install asphalt apron, change paint colors, and install tactile warning strips in walkway	\$ 13,231
CO 7	Add electrical in Training Room, remove trash encountered in trench for data cable, delete camera and monitor, add electric strike hardware in doorway 202A, and upgrade fire prevention system in Art Storage area	\$ 10,366
CO 8	Connect fire alarm system to campus panel, change electric for carpenter shop equipment, and add exhaust fan switch	\$ 8,040

##### **CERAMICS CENTER** Empire Contractors, Inc. – Contractor

CO 3	Delete toilet paper holders and hand dryers and delete the metal coping at the terrace canopy	(\$ 1,740)
CO 4	Relocate natural gas lines at exterior salt kilns	\$ 2,860
CO 5	Change water heater to electric, install booster transformer for ceramics equipment, add one guardrail, and make modifications to terrace louvers	\$ 4,220

**ATTACHMENT B**

**Summary of Construction Change Orders  
for Approval of the Finance/Audit Committee**

**Approval of the construction change orders in Attachment B (which require the approval of the Committee) is recommended.**

**BUSINESS AND ENGINEERING CENTER PROJECT**

**SUPPORT SERVICES BUILDING**

**Key Construction Company – Contractor**

CO 9	Install overhead garage door, card reader for opening, paved access drive, and associated work on the west side of the warehouse	\$34,452
CO 10	Install video camera and alarm system for security of art storage area	\$43,763



Bidder	Bid Category Base Bid			Alternate Bids										Full Totals		
	General Construction	Mechanical Construction	Electrical Construction	Alternate Bid No. 1 East Entry Tower	Alternate Bid No. 2 Meeting Room Bridge Enclosure	Alternate Bid No. 3 Underground Tunnel Extension	Alternate Bid No. 4 Supplemental Electrical and Data connections from adjacent buildings	Alternate Bid No. 5 Food Service fit-out and equipment	Alternate Bid No. 6 Supplemental site work and landscaping	Alternate Bid No. 7 Elevator #2	Alternate Bid No. 8 Millwork and Display Cases	Alternate Bid No. 9 Food Service fit-out on Level 2	Alternate Bid No. 10 Window Shades			
<b>General Construction</b>														\$0.00		LOW BID
Abel Construction Company	X													\$0.00		
Arc Construction Co., Inc.	X		\$10,510,900.00	\$1,595,370.00	\$207,000.00	\$251,652.00		\$537,500.00	\$218,700.00	\$245,400.00	\$228,310.00	\$130,500.00	\$105,100.00	\$14,030,432.00	\$11,507,052.00	
Deig Bros. Lumber & Construction Co., Inc.	X		\$10,300,000.00	\$1,582,000.00	\$225,000.00	\$150,000.00		\$503,000.00	\$215,000.00	\$252,000.00	\$218,000.00	\$157,000.00	\$107,000.00	\$13,709,000.00	\$11,178,000.00	
Empire Contractors	X		\$9,364,460.00	\$1,668,900.00	\$164,900.00	\$220,900.00			\$180,900.00	\$292,250.00	\$195,200.00			\$12,200,110.00	\$9,750,260.00	
Industrial Contractors, Inc.	X		\$10,580,000.00	\$1,670,000.00	\$321,000.00	\$291,000.00		\$506,000.00	\$158,000.00	\$289,000.00	\$219,000.00	\$163,000.00	\$101,000.00	\$14,298,000.00	\$11,698,000.00	
Peyronnin Construction Company, Inc.	X		\$10,690,000.00	\$1,600,000.00	\$333,333.00	\$233,000.00	\$8,000.00	\$530,000.00	\$222,000.00	\$257,000.00	\$199,000.00	\$168,900.00	\$115,000.00	\$14,356,233.00	\$11,786,333.00	
Precision Piping and Mechanical, Inc.	X													\$0.00	\$0.00	
Weddle Bros. Building Group, LLC	X		\$9,419,700.00	\$1,570,500.00	\$21,500.00	\$146,000.00		\$515,700.00	\$170,000.00	\$273,000.00	\$193,900.00	\$161,620.00	\$103,600.00	\$12,575,520.00	\$10,102,900.00	\$10,102,900.00
Williams Brothers Construction	X		\$10,668,000.00	\$1,525,000.00	\$200,000.00	\$280,000.00		\$444,000.00	\$172,000.00	\$330,000.00	\$245,000.00	\$160,000.00	\$103,000.00	\$14,127,000.00	\$11,592,000.00	
<b>Mechanical Construction</b>														\$0.00		
Deig Bros. Lumber & Construction Co., Inc.	X		\$1,784,070.00	\$122,300.00	\$15,280.00	\$7,636.00		\$2,020.00	\$430.00		\$3,479.00	\$870.00		\$1,936,085.00	\$1,809,006.00	\$1,809,006.00
Goedde Plumbing Heating, Inc.	X													\$0.00	\$0.00	
Harrell-Fish, Inc.	X													\$0.00	\$0.00	
Industrial Contractors, Inc.	X		\$2,024,900.00	\$80,000.00	\$20,600.00	\$7,900.00		\$6,800.00	\$1,000.00		\$4,000.00	\$8,600.00		\$2,153,800.00	\$2,060,200.00	
J. E. Shekell, Inc.	X		\$1,862,259.00	\$71,307.00	\$14,200.00	\$15,000.00			\$550.00					\$1,963,316.00	\$1,891,459.00	
Ray Haase Heating & A/C	X		\$1,949,323.00	\$80,000.00	\$13,364.00	\$12,200.00		\$6,300.00	\$400.00		\$5,000.00	\$1,800.00		\$2,068,387.00	\$1,981,187.00	
Peyronnin Construction Company, Inc.	X		\$1,826,000.00	\$83,200.00	\$7,800.00	\$4,250.00					\$2,395.00	\$480.00		\$1,924,125.00	\$1,838,050.00	
Precision Piping and Mechanical, Inc.	X													\$0.00	\$0.00	
Midwest Roofing and Sheet Metal	X		\$1,915,950.00	\$82,750.00	\$19,350.00	\$4,500.00		\$5,800.00	\$500.00		\$3,850.00	\$1,500.00		\$2,034,200.00	\$1,945,600.00	
<b>Electrical Construction</b>														\$0.00		
Alva Electric, Inc.	X		\$2,946,800.00	\$109,000.00	\$16,799.00	\$6,950.00	\$28,499.00		\$6,900.00		\$17,499.00			\$3,132,447.00	\$2,970,549.00	
Capital Electric	X		\$2,544,500.00	\$98,574.00	\$12,657.00	\$5,911.00	\$20,730.00	\$2,500.00	\$7,375.00	\$3,550.00	\$12,500.00	\$1,000.00		\$2,709,297.00	\$2,565,568.00	\$2,565,568.00
Deig Bros. Lumber & Construction Co., Inc.	X		\$3,048,643.00	\$128,210.00	\$12,775.00	\$9,905.00	\$44,215.00	\$12,415.00	\$9,809.00	\$4,000.00	\$18,000.00	\$2,774.00		\$3,290,746.00	\$3,083,738.00	
Gaylor Group	X		\$2,697,000.00	\$122,310.00	\$16,827.00	\$8,930.00	\$21,400.00		\$14,603.00	\$6,480.00	\$14,606.00	\$3,505.00		\$2,905,661.00	\$2,722,757.00	
Industrial Contractors, Inc.	X		\$3,742,269.00	\$113,708.00		\$12,806.00	\$34,219.00	\$3,850.00	\$25,737.00	\$8,593.00	\$21,052.00	\$15,798.00		\$3,978,032.00	\$3,758,925.00	
J. E. Shekell, Inc.	X		\$3,347,675.00	\$114,358.00	\$18,855.00	\$24,354.00	\$80,285.00		\$9,233.00	\$8,247.00				\$3,603,007.00	\$3,390,884.00	
Mel-Kay Electric Co., Inc.	X		\$2,745,000.00	\$105,000.00	\$12,000.00	\$7,100.00	\$40,000.00		\$15,100.00	\$6,500.00	\$18,800.00			\$2,949,500.00	\$2,764,100.00	
Precision Piping and Mechanical, Inc.	X													\$0.00	\$0.00	
Premier Electric, Inc.	X		\$2,783,000.00	\$106,400.00	\$19,000.00	\$9,500.00	\$23,000.00		\$16,000.00	\$8,000.00	\$8,000.00	\$4,500.00		\$2,977,400.00	\$2,811,500.00	
The State Group Industrial (USA) Limited	X		\$2,890,000.00	\$133,948.00	\$13,238.00	\$9,997.00	\$23,331.00	\$625.00	\$9,000.00	\$3,809.00	\$10,734.00	\$8,998.00		\$3,103,680.00	\$2,913,860.00	
<b>Combination Bids</b>														\$0.00		
Arc Construction Co., Inc.														\$0.00	\$0.00	
Deig Bros. Lumber & Construction Co., Inc.														\$0.00	\$0.00	
Industrial Contractors, Inc.														\$0.00	\$0.00	
<b>Low Bids Total</b>																\$14,477,474.00

PREPARED BY: David Goldenberg Director of Procurement and Risk Management

# Attachment D

## UNIVERSITY OF SOUTHERN INDIANA

### REPORT ON INTERNAL CONTROLS

Internal control refers to the design and use of controls that allow managers to administer current operations, plan for the future, and safeguard an organization's assets. Properly applied, good internal control procedures should insure the efficiency, effectiveness, and economy of any operation. The internal controls over the operational and financial activities of the University of Southern Indiana have been grouped into the following categories:

- **Accounting controls** relate directly to safeguarding assets and the reliability of the financial records. They address authorizations, approvals, and separation of duties between record keeping and asset custody.
- **Information system controls** are concerned with access to systems and data, the integrity of mission critical information, and the physical security of hardware and software systems. They include such controls as user authentication, backup and restore procedures, disaster recovery planning, and protection of equipment against theft and loss.
- **Administrative controls** are concerned with operational efficiency and adherence to policies. They generally include controls such as comparative analyses, performance reports, training programs, and quality control.

The controls identified in this report reflect management's representation of the internal control structure currently in place at the University. The controls in each subcategory are divided into those that conform to best practices and those that deviate from best practices. Deviations from best practices are not necessarily bad practices, but may reflect differences in our environment from that which existed when best practice standards were set. For example, technology has enabled some controls to be built into a process so that a separate step is no longer needed to provide proper control. This is only one form of compensating control. Other compensating controls are identified throughout the report.

#### ACCOUNTING CONTROLS

##### I. ACCOUNTS PAYABLE AND OTHER LIABILITIES

###### A. Conforms to Best Practices

1. Liability control accounts are reconciled with subsidiary records on a regular basis.
2. Accounts payable are maintained independently of cash receipts and disbursement functions.
3. Accounts payable and other liability adjustments are supported by documentation that has been properly reviewed and approved.
4. Procedures exist to facilitate payments to vendors in a timely fashion.
5. Procedures exist to prevent duplicate payments and payments for damaged goods.
6. Procedures exist to ensure proper credit for returned purchases.
7. Debit balances in liability accounts are reviewed regularly and reclassified at year end if appropriate.
8. Year end procedures ensure inclusion of all items purchased during the period.

###### B. Deviates from Best Practices

1. Receiving reports are not required for proof of delivery; therefore, the standard control of a three-way match of vendor invoice, purchase order, and receiving report does not exist prior to payment.
  - a. Compensating controls: Financial managers approve all items ordered via a purchase order. Also see compensating controls below.
  - b. Risk: Minimal. Only small dollar purchases are made outside the purchase order system.
2. Invoices up to \$5,000 are paid by negative confirmation if a purchase order exists and the invoice amount agrees (within reason) with the purchase order amount.
  - a. Compensating controls: Financial managers are notified of invoices scheduled for payment and given 15 days to notify AP of a reason why the vendor should not be paid. If no response is received from the financial manager, or his/her alternate if the financial manager is absent, payment is processed as scheduled.

- b. Risk: Minimal. Financial managers approve all items ordered via a purchase order.

## II. ACCOUNTS RECEIVABLE

### A. Conforms to Best Practices

1. Accounts receivable are maintained independently of cash receipts and disbursement functions.
2. Bad debt write-offs, credit memos, and allowances are approved independently of processing, recording, and collecting.
3. Individual accounts are independently reconciled with the control account on a regular basis.
4. Aged accounts, and accounts with credit balances, are reviewed periodically.
5. Measures exist that encourage prompt collection of student accounts receivable.
6. Procedures exist for follow-up and collection of delinquent accounts.
7. Disputed liabilities are handled by persons other than those receiving payment.
8. Completed invoices are controlled and properly accounted for.
9. Adequate control exists over the mailing of statements to prevent interception prior to mailing.

### B. Deviates from Best Practices

1. Account receivable balances have not been independently confirmed on a periodic basis.
  - a. Compensating controls: None
  - b. Risk: Not yet determined.
2. Only one person can build the billing tables in Banner (the University's enterprise management system), test them, and prepare the student billings each semester.
  - a. Compensating controls: None. A solution is currently being developed.
  - b. Risk: Not yet determined.
3. Follow-up and collection on delinquent receivable accounts not performed on regular or timely basis since conversion to Banner.
  - a. Compensating controls: Banner delinquency codes will help with catch up.
  - b. Risk: Not yet determined.

## III. CASH DISBURSEMENTS

### A. Conforms with Best Practices

1. Check or Electronic Disbursements
  - a. Adequate separation of duties exists between the approval and payment functions.
  - b. All checks are made payable to specific payee.
  - c. Advance signing of checks is impossible because of software security.
  - d. All disbursements are properly authorized and supported by appropriate documentation, which is reviewed before checks are issued.
  - e. All bank accounts and check signatures are properly authorized; check signers are adequately insured.
  - g. Procedures provide for immediate bank notification when an authorized signer of checks changes duties or resigns.
  - h. The supply of blank checks is adequately controlled and secured.
  - i. Voided checks are properly mutilated and held for inspection; old outstanding checks are voided after one year.
  - j. Vouchers, or other approved documentation, are prepared for all expenditures, including wire transfers and Automated Clearing House (ACH) debit entries.
  - k. Facsimile signature is electronically stored in software and applied during check run process.
  - l. A firm procedure establishes the conditions under which disbursements can be made.
  - m. Each bank account is under a separate ledger control.
  - n. Bank accounts are reconciled monthly by a person independent of cash functions.
  - o. The sequence of check numbers are accounted for when reconciling bank accounts.
  - p. The check production system does not omit check sequence numbers during printing or in the event of printing errors.
  - q. A positive pay process is used to verify checks produced to checks processed by the bank for clearing. Exceptions identified by the bank require approval by USI before processing.
  - r. Cancelled checks are returned from the bank electronically which prevents physical alteration after processing.

- s. Bank software requires user ID, a password, and a random number generator provided by the financial institution to approve electronic disbursements.
  - t. Direct deposit files are generated by the Computer Center staff who do not have responsibility in the preparation and disbursement process
2. Petty Cash Disbursements
- a. Petty cash funds are properly authorized, the responsibility of only one person, and are properly safeguarded.
  - b. Petty cash vouchers are signed by the person receiving cash, prepared in ink, and required for each expenditure.
  - c. Petty cash disbursements are supported by original receipts verifying the amount disbursed.
  - d. Reimbursement vouchers to replenish fund are approved by a responsible employee who has no daily cash handling responsibilities.
  - e. Vouchers and attachments are properly cancelled to preclude reuse.
  - f. Petty cash funds are limited to expenditures not exceeding a fixed amount; variances to that amount require special approval.
  - g. Petty cash fund balances are adequate for the activity's needs.
  - h. The funds are verified by surprise counts.
3. Travel Disbursements
- a. The authority for approval of travel requests is established at all organization levels.
  - b. Travelers are educated regarding the institution's travel regulations.
  - c. Travel is supported by an approved travel request form with the exception of local travel within a radius of 50 miles and no overnight stay.
  - d. The business purpose of travel is stated on the face of the travel request.
  - e. Cash travel advances are limited in scope and tightly controlled, and original receipts are required to reconcile travel advances.
  - f. The appropriate financial manager or approved alternate approves all travel reimbursement vouchers.
  - g. All travel vouchers are independently reviewed in detail for allowability and reasonableness.
  - h. Travelers are required to provide original receipts for all travel expenditures, and unauthorized personal travel expenses are excluded from reimbursement.
  - i. Travel plans are made sufficiently in advance to obtain the most favorable transportation rates.
  - j. Procedures are in place to govern student and field trip travel.
- B. Deviates from Best Practices
- 1. Endorsements on cancelled checks are not periodically examined nor are paid checks randomly scrutinized for suspicious and irregular features. The check volume is so large that this would be a daunting task. It is doubtful that such scrutiny would result in identifying an altered or a fraudulently endorsed check.
    - a. Compensating controls: A great number of payments are now being made electronically rather than by paper checks. Check stock has security features which make it difficult to alter. The bank provides 'positive pay' service which catches odd check numbers or mismatched amounts with check number.
    - b. Risk: Minimal.

#### IV. CASH RECEIPTS

- A. Conforms with Best Practices
- 1. Cash receipts are maintained independently of accounts receivable, accounts payable, and check disbursement functions.
  - 2. Cash receipts are promptly recorded using pre-numbered receipts, on-line computer numbered receipts, or cash registers by an individual designated to receive cash.
  - 3. Cash register/cashiering procedures reflect proper daily check-out and documentation.
  - 4. Customer receipts (computer generated or multi-copy hand written) are dated, numerically controlled, and identifiable to a specific cashier.
  - 5. Employees connected with the cash receipts function rotate duties periodically.



6. Cash overages/shortages for each cashier are maintained and recorded on the books.
7. Cash receipts are posted daily to income or subsidiary accounts receivable records.
8. Cashiers are provided separate cash drawers to establish accountability. These drawers are locked during the cashier's absence.
9. Cash receipts are deposited intact on a daily basis; deposits are verified by means of a bank receipt or online access to bank account activity.
10. Adequate facilities are provided for the safeguarding of cash prior to deposit.
11. Safe combinations and keys to cash boxes/files are restricted to an essential number of employees; combinations and locks are changed at each personnel change.
12. Checks returned by the bank are posted to subsidiary accounts receivable records; notification letters are sent to the payor requesting prompt redress.
13. All persons handling cash are adequately insured.
14. All credit card transactions are processed by a third party vendor that meets the payment card industry's data security standards governing cardholder information.

NOTE: The above cash receipts controls apply to the Bursar/Cashier department. They may or may not be in place at all locations that handle cash.

B. Deviates from Best Practices

1. The mail is not opened by someone independent of cashiering or accounts receivable duties. One accounts receivable staff opens the mail daily. This person is also a backup cashier.
  - a. Compensating controls: Mail is opened in a secure and controlled environment and in the presence of other people. A restrictive endorsement is immediately stamped on the check.
  - b. Risk: Minimal.

V. INVESTMENTS

A. Conforms with Best Practices

1. An investment policy has been established by the Board of Trustees.
2. Changes in types of investments in the portfolio are approved in accordance with the investment policy.
3. Investments are purchased and sold only upon proper authorization.
4. Original papers evidencing purchases and sales are properly filed.
5. An independent safekeeping agent is utilized; investments are either in a safe deposit box or in the University vault.
6. Investment documents are under the control of a responsible official as custodian.
7. A record is maintained for each investment, including cost, description, purchase date, maturity date, interest rate, and identifying number.
8. A record of investment income is maintained, and accruals are recorded as investment income is earned.
9. Investments are examined periodically and reconciled to controlling accounts.
10. Earnings are reconciled periodically with published financial records.
11. Confirmations are obtained from outside holders of investment documents.

B. Deviates from Best Practices

1. Procedures do not require that more than one person be present during inspection of investments held in the safe deposit box or the University vault.
  - a. Compensating controls: The bank maintains a record of who visited the safety deposit box on a specific date.
  - b. Risk: Minimal.
2. All persons having access to investments are insured, but the level of coverage may not be adequate if a successful theft should occur.
  - a. Compensating controls: Most investments (CDs, federal paper) are registered in the University's name. If stolen or destroyed, USI would be able to collect. Some government securities are held in the name of the nominee bank and insured by policies of the financial institution or guarantees of the U.S. government.
  - b. Risk: Minimal.

## VI. PURCHASES

### A. Conforms with Best Practices

#### 1. Purchase Order Processes

- a. Purchasing policies are defined by written procedures.
- b. Purchases, other than those from petty cash, by procurement card, or below the minimum dollar threshold, are made on properly approved orders.
- c. The use of confirming (after the fact) purchase orders is documented and monitored.
- d. System approval queues requiring financial manager approval are required to submit purchase requisitions for processing.
- e. Adequate separation of duties exist in connection with issuing approved purchase orders, placing orders with vendors, approving vouchers for payment, processing approved vouchers, and disbursing funds.
- f. Policies provide for the assignment of responsibility for final purchasing decisions at the appropriate level.
- g. All purchase order numbers are system generated and accounted for.
- h. Leasing procedures insure compliance with statutory purchasing regulations, as well as University rules and regulations.
- i. A system of competitive bidding is used.
- j. Long-term contracts are under adequate control.
- k. There is a policy statement with regard to conflicts of interest, including employee-vendor relationships.

#### 2. Procurement Card Processes

- a. All procurement cards policies and procedures have been approved by authorized management.
- b. All cardholders are provided with an up-to-date copy of the policies and procedures, and are required to undergo training before their cards are activated.
- c. All cards are issued in the name of individual employees to fix accountability.
- d. All cardholders are required to sign a cardholder's agreement that states terms and conditions.
- e. New and replacement cards are issued inactive, distributed in a secure manner, and only activated upon action by the cardholder.
- f. Cardholders are held personally responsible for unauthorized or personal purchases, and disciplinary measures are in place for card misuse/abuse.
- g. Card usage is monitored for personal use, and charges are examined monthly for authorization, propriety, and purchasing limits.
- h. Monthly and transactional purchase limits are built into the card system software.
- i. Pre-defined Merchant Category Classification Codes (MCC) are used to eliminate some merchants from card purchases.
- j. A log of card purchases by person and by vendor is retained several months in the online system.
- k. A process exists for reporting and deactivating lost or stolen cards, and liability for fraudulent use is limited between the time of the card being stolen and the time it is reported.
- l. All card purchases are required to be signed-off on by the financial manager of the charged account.
- m. All purchases are required to be supported by original receipts including vendor's name, date of purchase, total amount, itemized description of each item purchased, and business purpose if not evident.
- n. Cardholders are required to reconcile their credit card statement to actual receipts on a monthly basis.
- o. Card usage is monitored for "stringing," i.e., breaking down one large purchase into several smaller purchases to circumvent purchase authorization limits.
- p. There is an established procedure for dealing with disputed transactions with the card issuer.
- q. All cards have expiration dates.
- r. There is a procedure for retrieving the procurement card when an employee leaves the organization.

B. Deviates from Best Practices

1. Confirming (after the fact) purchase orders that are not initiated by the purchasing department have not been subject to review for best vendor or best price comparisons.
  - a. Compensating controls: Departmental budgets and financial manager authority
  - b. Risk: Unknown.
2. Blanket orders are issued to frequently used vendors for "miscellaneous supplies" so that what is being purchased is not known in advance. If known, some items could be bid out for better prices.
  - a. Compensating controls: Departmental budgets and financial manager authority
  - b. Risk: Unknown.

## VII. PAYROLL

A. Conform to Best Practices

1. Policies regarding time worked, vacations, sick leave, holidays, and other employee benefits are published in the USI handbook and accessible via the web site.
2. Written approval is required for employee additions and deletions from the payroll, changes in pay rates, and payroll deductions.
3. Time sheets and pay vouchers are approved by someone in authority.
4. There is a segregation of personnel and payroll functions.
5. Procedures exist to ensure that all employees are bona fide, and that employees do not receive more than the authorized salary payment.
6. Payroll checks are either direct deposited to employee's bank or distributed by the Cashier's office.
7. Identification is required before receiving paycheck from the cashier.
8. Procedures exist for the control and disposition of any old, outstanding payroll checks.
9. Payroll office employees are cross-trained on many duties to cover absences.
10. Vacation, sick leave and compensating time off are properly documented and controlled.
11. The payroll bank account is maintained on an imprest basis and reconciled by someone having no payroll duties.
12. Blank payroll checks are adequately controlled and safeguarded.
13. Procedures exist to prevent employees from receiving pay other than through properly approved and processed payroll procedures for services performed.

B. Deviates from Best Practices

1. No formalized record retention policy has been developed for payroll or personnel source documents.
  - a. Compensating controls: Records are retained for longer than needed rather than being destroyed too soon.
  - b. Risk: Unknown. A retention policy lessens burden to produce records in a legal issue from a period earlier than the period stated in a retention policy.

## VIII. EQUIPMENT AND FIXED ASSETS

A. Conforms to Best Practices

1. Capital expenditures are authorized by appropriate officials.
2. Equipment acquisitions are originated by requisitions that show description, estimated cost, and accounts to be charged.
3. Equipment additions are controlled by a budget. Variations between budget and actual costs require financial manager approval.
4. A policy exists that differentiates between expenditures to be capitalized and those to be expensed.
5. Identifying information (tag or bar code) is placed on equipment after it is installed or placed in its intended location and removed from equipment prior to disposal.
6. Detailed subsidiary records of equipment are maintained, reconciled to the general ledger by fund, and adjusted when equipment is disposed of or transferred.
7. Physical inventories of all equipment are taken periodically. An inventory of large dollar items is taken at least annually.
8. Inventories are tested periodically by an official having no responsibility for the inventory.
9. A computerized preventive maintenance program is used to schedule and identify inspections and

- maintenance for major heating and cooling systems. Other equipment is covered by maintenance agreements with vendors.
10. Equipment is reviewed periodically for the purpose of determining adequate insurance coverage.
  11. A procedure exists of identifying and disposing of unused or obsolete equipment. An asset control personnel authorizes the disposal and appropriate paperwork is completed.
  12. The sale, transfer, scrapping or dismantling of equipment requires written approval.
  13. Surplus equipment sales are publicized, use a computerized anonymous bidding process for purchase, and are reviewed by internal audit.

NOTE: The above policies and procedures apply to equipment under the control of Purchasing & Risk Management and the Physical Plant. Different policies and procedures are in place for the equipment controlled by the Computer Center.

## **INFORMATION SYSTEM CONTROLS**

### **I. DATA OPERATIONS**

#### **A. Conforms to Best Practices**

1. All operations tasks including program and equipment maintenance, computer system upgrades, and testing are scheduled in advance.
2. Operations procedures include recording software and hardware problems, management of the tape/cartridge library, cleaning and performing preventive maintenance on the computer equipment (vendor contract), powering up and shutting down the equipment, and running and correcting jobs.
3. Backups of all systems are performed on a daily basis. Backup procedures include the backup of master files, tables, and transactions; the backup of application programs; the backup of systems software; the backup of automated log data; the labeling and identification of backup files; the retention and timely rotation cycle of backup files; the storage of application, system software, disaster recovery plan, and other system operations documentation at a secure location away from the computer center; system testing of critical backup tapes for readability; cross-training of data processing staff; and removal of backups to a secure off-site storage location.
4. Cross training of staff includes the rotation of operators on each application and operations function and more than one person being familiar with the systems software.
5. A written disaster recovery plan exists which addresses a predetermined priority for application processing, the minimum computer configuration, data and application software, physical facilities, security, etc., necessary for processing critical systems, and personnel responsibilities.
6. All abnormal terminations are logged, and applications have checkpoint and restart procedures which allows processing to continue from the record of the last checkpoint before an abnormal termination occurred.

#### **B. Deviates from Best Practices**

1. Although a written disaster recovery plan exists, it has not been evaluated or updated since 2005,
  - a. Compensating controls: None identified.
  - b. Risk: Not yet determined.

### **II. NETWORK ENVIRONMENT**

#### **A. Conforms to Best Practices**

1. Access by individuals to on-line systems is controlled using passwords and single log-on restrictions.
2. Password controls consist of password change required every 60 days; 6 character minimum length and must be a combination of alpha and numeric characters; password does not appear in clear text during log-on or on reports; password encrypted or password table secured; and lock-out after three unsuccessful log-on attempts. Passwords are assigned to individual users rather than user groups.
3. Security software is in place to detect or prevent unauthorized access to the network environment, and security patches are kept up to date.
4. Network access is terminated when the computer center is notified of employee terminations.

5. All drives and files on the network are scanned for viruses in real time, and virus software is updated as new data is available.
6. There is a firewall protecting the network environment through which all traffic must pass, and all dial-up users must provide authentication to get within the firewall.
7. There are controls in place to prevent denial of service attacks, and to detect intrusion attempts and unusual activity.
8. Access to data is restricted on a "need to know" basis, and physical access to data is restricted.
9. Security logins are required for access to the wireless network and wireless access to the internet.
10. Wireless access points are properly configured to restrict network access, and the network is monitored for unauthorized access points.
11. Security controls are in place to restrict wireless network access through intrusion detection systems, by network segregation, and by requiring users to register for access.

B. Deviates from Best Practices

1. Network administrator passwords do not expire. They are changed on an irregular schedule at least once a year or whenever there are staff changes.
  - a. Compensating controls: Complexity required for network administrator passwords
  - b. Risk: Medium.
2. There is not auto log-off from the network due to inactivity. Some employees remain logged onto the network for extended periods or seldom log off. The workstation is then available for anyone to access in the employee's absence.
  - a. Compensating controls: Other programs accessed from the network do have auto log-off - Banner enterprise management system, 30 minutes; Xtender document imaging system, 20 minutes; and Cognos report writer, 60 minutes.
  - b. Risk: Not yet determined.

### III. PHYSICAL SECURITY

A. Conforms to Best Practices

1. Access to the computer room is limited to operators and other employees whose job duties require physical access to it.
2. Unauthorized access to the computer room is restricted by the use of combination locks.
3. Physical access to the tape/cartridge archives is restricted to the librarian and others only when authorized and accompanied by the librarian.
4. Emergencies can be reported by using an alarm pull box that sounds in the computer room and in the control room in the physical plant.
5. Periodic drills reinforce emergency evacuation procedures.
6. Techniques exist to detect and extinguish fire.
7. Warning sensors exist to alert for water in the computer room and network server area.
8. Backup storage exists in both on-campus (weekly tapes) and off-site locations.

B. Deviates from Best Practices

1. The computer room and network room are located in the lower level of the Orr Center. This area has been subject to water leakage in the past, both from ground water and cooling equipment failure. Flooding from plumbing failures is also a possibility.
  - a. Compensating controls: Work has been done to improve ground water drainage around the building and warning sensors have been installed.
  - b. Risk: Unknown.

### **ADMINISTRATIVE CONTROLS**

I. GENERAL

- a. The University has a statement of mission and objectives.
- b. The University is governed by a Board of Trustees appointed by the Governor of the State of Indiana.
- c. There is a current organizational chart in use which reasonably fixes the responsibility of key personnel.
- d. A formalized internal policy and procedures manual exists and is updated regularly.
- e. The formalized policy includes a code of ethics, a policy on fraud and the reporting thereof, and addresses conflicts of interest.

- f. Written job descriptions exist for all employee positions.
- g. A budgetary control system is in place and monitored regularly.
- h. Financial reports provide complete and timely information.

## II. MANAGEMENT REVIEW

- a. All major channels of communication are utilized effectively.
- b. Fiscal authority has been formally delegated to specific management personnel.
- c. Fiscal responsibility exists at all management levels.
- d. Employees are evaluated regularly.
- e. Managers/supervisors review the evaluations with their employees.
- f. Management provides in-house employee training and educational programs that are job oriented.
- g. Management encourages participation in continuing professional education activities provided by outside organizations.
- h. Management promulgates and upholds ethical practice and behavior in all endeavors on behalf of the University.

### **DISCLAIMER**

No list of internal controls can be all-inclusive, nor can it reveal all the dimensions of any statement regarding internal control. Even though the above list represents the standard operating controls and practices of this university and its employees, there will occasionally be deviations from these controls and practices. Sometimes the deviations are warranted by the circumstances; sometimes by thoughtlessness. To our knowledge, there has not been a willful violation of internal controls that resulted in fraud or personal gain.

**University of Southern Indiana  
Internal Audit Report Summaries  
Calendar Year 2008**

AUDIT NAME				
OBJECTIVE	OBSERVATIONS	RECOMMENDATIONS	MANAGEMENT RESPONSE	STATUS
<p><b>Time Worked vs. Time Reported</b> (1.) Determine the amount of time worked versus the amount of time reported on the official University time sheet.</p>	<p>An unofficial <i>Overtime Tally</i> log was being maintained to track flex time hours for six support staff in the area under review. Two staff redeemed their flex hours within one work week per policy, the remaining staff carried hours across pay periods, but only one person did so regularly and frequently. Time sheets submitted to payroll always reflected a normal work week rather than the actual hours worked.</p>	<p>Review the University policy with support staff and their supervisors, always report actual hours worked to payroll.</p>	<p>Meetings were conducted by the provost and HR director with support staff and supervisors. The policy was reviewed and explained. They emphasized the requirement to report actual time worked on all time sheets from that point forward.</p>	<p>Completed</p>
<p>(2.) Determine if employees have been fairly compensated or granted the appropriate amount of time off.</p>	<p>All six employees had more hours worked than they had been compensated for at the time of the review.</p>	<p>Payroll staff should calculate the number of hours and pay that each employee is entitled to. Give employees option of compensated time off or overtime pay.</p>	<p>Payroll made the recommended calculations. The payroll manager and the HR director met with each person and documented their choice of overtime pay or compensated time off.</p>	<p>Completed</p>
<p>(3.) To evaluate if fraudulent activity occurred.</p>	<p>We found no indications of fraudulent activity. The practice in place was a result of supervisor and administrative misunderstanding of the University's policy on flex time reporting.</p>	<p>None</p>	<p>NA</p>	<p>NA</p>
<p><b>Banner Financial Aid (FA) Security Access</b> (1.) To evaluate the security access granted to Student Financial Assistance staff to:</p>	<p>Generally, users are assigned to roles that are closely aligned with their functional areas and job duties, but some have more access than needed.</p>	<p>Review and scale back role access that was initially granted but now found to be excessive. Schedule time for security maintenance to review user access and its appropriateness.</p>	<p>Agreed with recommendations. Plan to perform periodic reviews of security access every six months after initial review.</p>	<p>In progress: June 2009</p>
<p>a. determine if access is appropriate for related job responsibilities,</p>	<p>Several users had unnecessary update capability for a General Student module form.</p>	<p>Trim user access determined to be excessive.</p>	<p>Access for all FA classes was revised to 'query access only' for the form in question.</p>	<p>Completed</p>
<p>b. confirm that excessive or conflicting update authority does not exist, and</p>	<p>Separation of duties is adequate and numerous compensating controls are in place. Data entry logs are reviewed only when a known problem exists.</p>	<p>Schedule periodic reviews of key field log entries for unusual activity even though a known problem has not been identified.</p>	<p>Periodic reviews will be performed by the Assistant Director on the first day of every month.</p>	<p>Completed and ongoing</p>
<p>c. ensure that proper separation of duties exists.</p>	<p>A few non-departmental staff have inappropriate update capability for certain year-specific forms.</p>	<p>Remove inappropriate update capability.</p>	<p>Inappropriate access was corrected as of 7/21/08.</p>	<p>Completed</p>
<p>(2.) Evaluate security access granted to staff in other departments to determine appropriateness of access and update capabilities.</p>	<p>Two user classes have no members.</p>	<p>Evaluate continuing need.</p>	<p>Null classes will be populated for the automation of federal workstudy payroll entries for FY08-09.</p>	<p>Pending: April 2009</p>

**University of Southern Indiana  
Internal Audit Report Summaries  
Calendar Year 2008**

AUDIT NAME				
OBJECTIVE	OBSERVATIONS	RECOMMENDATIONS	MANAGEMENT RESPONSE	STATUS
(3.) Review access approval procedures and controls.	Access policies and procedures are in place, understood, and followed by the security administrator, but they are not in written form.	Record the access policies and procedures in writing.	Policies and procedures will be documented.	In progress: June 2009
<b>Banner Accounts Receivable (AR) Security Access</b>				
(1.) Evaluate security access granted to Bursar/ Cashier Office staff to  a. determine if access is appropriate for related job duties,	In general users are assigned roles that are closely aligned with their functional areas and job duties. Roles are adequately limited based on needed access for specific tasks or procedures. Some access duplication/fragmentation exists between Banner Finance and AR modules for some users.	Analyze user access and consolidate AR access into AR classes. Eliminate duplicated/fragmented access between Finance and AR.	Agreed with recommendations.	Completed
b. confirm that excessive or conflicting update authority does not exist, and	Excessive or conflicting update capability is not an issue for most users, but there are superusers with extensive update access in both Banner Finance and AR modules.	Evaluate and trim the access of Banner Finance superusers. Adjust AR user's unrestricted charge/ payment posting to correct classification - supervisory or restricted.	Agreed with recommendations.	Completed
c. ensure that proper separation of duties exists.	Separation of duties is enforced by software access restrictions for most. Some duties are separated by policy enforcement with management oversight acting as a detective control.	None	NA	NA
(2.) Evaluate security access granted to staff in other departments to determine appropriateness of access and update capabilities.	Most users external to AR have very limited and query only access. Sodexo (contractor) staff has been granted access to carry out student meal plan functions. USI dependent on Sodexo to notify when users change.	Pro-actively contact areas with non-USI employee users periodically to verify employment and continuing access need.	HR is tracking this information. We are working with them to obtain the needed information.	Completed and ongoing
(3.) Review access approval procedures and controls.	The procedures are documented in detail including flow charting for the approval process.	None	NA	NA
<b>Federal Grant Compliance</b>				
1. Verify compliance with federal OMB circular and agency guideline requirements.	Compliance was strong for many federal requirements, but we found significant opportunity for improvement in time and effort reporting and in establishing allowability for some costs and indirect cost recovery.	Involve relevant departments in devising a process that results in an accurate certification of effort while minimizing payroll reallocations.  Verify that supporting documentation specifically establishes why any generally unallowable expenditure is allowable in each instance.	Proposed a meeting with all relevant persons to work out a solution for the time and effort reporting issue.  A new daily report from Cognos summarizes all requisitions entered against restricted funds. This tool will provide opportunities to communicate with departments to clarify the allowability of purchases before they transpire.	Pending: March/April 2009  Completed and ongoing



**University of Southern Indiana  
Internal Audit Report Summaries  
Calendar Year 2008**

AUDIT NAME				
OBJECTIVE	OBSERVATIONS	RECOMMENDATIONS	MANAGEMENT RESPONSE	STATUS
2. Verify compliance with the specific federal agency grant agreement or contract terms.	Per the grant guidelines, facilities and administrative (F&A) costs were limited to a percentage of direct costs. The F&A rate for this grant was charged on the basis of the approved budget rather than actual costs. This resulted in a higher recovery than should have been taken.	Charge F&A costs as a percentage of actual expenditures, not budgeted amounts.	All grants will be reviewed for compliance, and a new monthly reconciliation of F&A costs will document that all amounts are charged based on the percentage outlined in the agreements.	Completed and ongoing
3. Verify conformance with institutional-sponsored agreement policies, procedures, and guidelines.	Policies and procedures are sufficient; however, there are inconsistencies between practice and internal policies and procedures governing effort reporting.	Revise time and effort reporting policy or alter practice to achieve agreement between policy and practice.	The policy will be amended to reflect current practices.	Pending: June 2009

## **Audit Report Time Worked vs. Time Reported**

### **BACKGROUND**

From an exit conference with a terminating support staff who had been employed in the College of Nursing and Health Profession, the HR director learned that employees in that area may have been instructed to keep two sets of time-keeping records: one of actual hours worked and another that was reported on the time sheets, which were submitted to payroll for processing. This information was shared with the provost, who then met with the dean of the College and the program directors to determine the reliability of the claim. From these meetings it was evident that there was some misunderstanding all around about the distinction between 'flex time' and compensatory time, and the importance of recording actual hours worked on the official University timekeeping document. Internal Audit was brought in to review the past year to determine the level of misreporting.

### **AUDIT OBJECTIVES**

1. To determine the amount of time worked versus the amount of time reported on the official University time sheet.
2. To determine if employees have been fairly compensated or granted the appropriate amount of time off.
3. To evaluate if fraudulent activity occurred.

### **AUDIT SCOPE**

In the course of the review, we analyzed the time reported on an unofficial *Overtime Tally* log maintained by some employees in the College, reviewed correspondence regarding absences and flexible hours worked which was maintained in a centrally located three-ring binder, and reviewed the time reported to payroll for the period beginning January 2007 through the pay period ending March 7, 2008. We also interviewed the dean of the College to obtain her understanding of the practice and the reason for its existence.

### **AUDIT SUMMARY AND OBSERVATIONS**

The practice of logging actual hours worked versus hours turned in on the time sheet began as a means to document flexible work schedules. The *Overtime Tally* log provided a place for the date, an explanation of what occurred, time reported on the time sheet, actual hours worked, columns for plus/minus hours designated as "school requested" or "employee requested", a running balance column, and a column where the supervising program director initialed his/her approval.

The purpose was to allow employees to work flexible hours and to avoid unnecessary overtime. Flex time was attractive because there were times when events or circumstances caused staff to be on duty outside normal working hours, and they could compensate for that by taking time off at other times. The running balance on the log helped each employee to keep track of whether they needed to take time off or work extra. However, on the official time sheet the employee would report a normal work day for each day of the time period, resulting in a full paycheck that otherwise might have been short or might have included overtime.

The University's policy on flexible time is found in the handbook, Item E.8, under Compensatory Time and states

*"An altered work schedule within a given work week should not be confused with reporting compensatory time for use in future work weeks. If an employee works fewer hours on one day to offset longer hours on another day in the same work week, there would be no compensatory time accrued in that work week, as long as the schedule change results in 37.5 (or fewer) hours reported. Such schedule adjustments within a given work week must be approved by the employee's supervisor, and the employee must report actual time worked each day on the timesheet."*

Of the twelve support staff employees in the College of Nursing and Health Professions area, only six employees maintained the *Overtime Tally* log during the time under review. Of those six, two performed their

altered work schedule within a given week most of the time rather than spreading it over a two-week pay period or beyond. Four employees spread their flex time schedule beyond one week or beyond one pay period. And, of these four, only one employee did this on a frequent and regular basis.

We found no evidence that anyone was trying to falsify records. As mentioned above, only half of the employees participated in the plan, and then not in a consistent manner. Participating employees and program directors were operating under the impression that this was an acceptable arrangement based on the direction they had received on how to control overtime hours while still maintaining coverage for vacations, sickness, or special events. The dean accepted responsibility for not paying closer attention to how the documentation was being reported to payroll and for not realizing that the flexible-hours method being practiced by some employees was outside University policy and procedures.

#### **MANAGEMENT CORRECTIVE ACTIONS**

- The provost met with the program directors and explained the inappropriateness and seriousness of the work time reporting processes that were being used by some of the CNHP staff.
- The HR director met with the staff and outlined the University policy on reporting time and explained the differentiation between flex time and comp time.
- The payroll manager calculated the overtime hours and the dollar amount due to each employee who had remaining, unpaid hours from the period under review. Each employee was given the choice to receive compensatory time off or overtime pay.
- The provost met with all the deans, directors, and chairs to review the policy on time reporting and emphasized the need to follow policy at all times.

#### **CONCLUSION**

The corrective actions taken should strengthen controls over time reporting for the College of Nursing and Health Professions as well as all other academic areas.

## Audit Report Banner Financial Aid Security Access

### RESULTS AT A GLANCE

AREAS	RISK MITIGATION			
	Adequate Controls & Practice	Opportunity for Minor Improvement	Opportunity for Moderate Improvement	Opportunity for Significant Improvement
<b>Audit Objectives:</b>				
Appropriate access for related job duties				
Excessive or conflicting update authority				
Proper separation of duties				
Access granted to non-Financial Assistance department users				
Approval process procedures and controls				

### EXECUTIVE SUMMARY

#### BACKGROUND

The Department of Internal Audit has completed an audit of the SunGard Banner Financial Aid system access security. The security maintenance function at USI for the Financial Aid system of the SunGard Banner Student module is separate from security maintenance for the General Student/Admission and Student Accounts Receivable systems. General Student/Admission was covered in a previous audit and Accounts Receivable security access for the Student module will be examined at a later date.

The Assistant Director of Student Financial Assistance acts as the security administrator and data manager for the Financial Aid portion of the Banner Student module. Access requests that originate within the Financial Assistance office are typically sent directly to the Assistant Director. Requests from other departments are normally sent to the Director and forwarded upon approval to the Assistant Director. The security administrator controls access to Banner by assigning authorized users to a user role or roles, or by granting direct access to specific Banner objects (forms, processes, etc.). Each user role has access to a set of forms, reports, and processes within the Banner application. The access granted for most forms, reports, or processes can either be maintenance, which is updating capability, or query, which is view only access.

Users should be granted sufficient access to perform all job duties, but access should be as limited as possible to minimize the possibility of fraud or the exposure of sensitive or confidential information. Restricting access to this information also reduces the risk of the institution violating federal laws or regulations including the Family Education Rights and Privacy Act (FERPA).

## AUDIT OBJECTIVES

The objectives of the audit are as follows:

1. To evaluate the security access granted to Student Financial Assistance employee users for SunGard Banner Financial Aid to:
  - a. determine if access is appropriate for related job responsibilities,
  - b. confirm that employees do not have excessive or conflicting update authority, and
  - c. ensure that proper separation of duties exists.
2. To evaluate the security access granted to non-Student Financial Assistance department users of Banner Financial Aid to determine the appropriateness of access and any update capabilities.
3. To review the access approval procedures and controls to determine how access is granted, how specific form access needs are determined and approved, and how update form conflicts are resolved.

## AUDIT SCOPE

We examined the following regarding Banner Financial Aid access security:

- Security documentation for the Banner Financial Aid system
- Reports from the database administrator for form, report, and process security and for user role security as of January 22, 2008
- User roles for appropriateness of form, report, and process access
- Appropriateness of user role assignments to position and general job duties for all users
- The process by which access is granted to the Banner Financial Aid portion of the Student module
- How the extent of access is determined

## AUDIT SUMMARY

We did not discover any major security issues during our review. Generally, users are assigned to roles that are closely aligned with their functional areas and job duties. Time constraints have prevented a thorough review by the security administrator of the security access granted during the initial go-live of Banner Financial Aid in February 2006.

### Opportunities for minor improvement exist for each of the following audit objectives:

- Appropriate access for job related responsibilities
  - Action Plan Task: Review and reclassify employees' access to reflect appropriate security views.
  - Action Plan Task: Review security access every six months.
- Proper separation of duties
  - Action Plan Task: Review selected key field log entries on the first working day of each month.
- Access granted to non-Student Financial Assistance department users
  - Action Plan Task: Adjust internal audit and computer center classes to remove update capability.
  - Action Plan Task: Populate classes for the automation of FWS wages for the 08/09 award year.
- Access approval procedures and controls
  - Action Plan Task: Record the access policies and procedures in writing.

### Opportunity for moderate improvement exists for the following audit objective:

- Excessive or conflicting update authority
  - Action Plan Task: Revise all FA classes to query only access for form SPAIDEN.

## **CONCLUSION**

The security administrator is very experienced and knowledgeable. She understands the Banner Financial Aid system capabilities and grants appropriate access to users. The completed actions will strengthen controls over access to the Banner Financial Aid system.

## Audit Report Banner Accounts Receivable Security Access

### RESULTS AT A GLANCE

AREAS	RISK MITIGATION			
	Adequate Controls & Practice	Opportunity for Minor Improvement	Opportunity for Moderate Improvement	Opportunity for Significant Improvement
<b>Audit Objectives:</b>				
Appropriate access for related job duties				
Excessive or conflicting update authority				
Proper separation of duties				
Access granted to non-Bursar/Cashier's Office users				
Approval process procedures and controls				

### EXECUTIVE SUMMARY

#### BACKGROUND

The Department of Internal Audit has completed an audit of the SunGard Banner Accounts Receivable system access security. The security maintenance function at USI for the Accounts Receivable system of the SunGard Banner Student module is separate from security maintenance for the General Student/Admission and Student Financial Aid systems. General Student/Admission and Financial Aid access security were covered in previous audits.

The Bursar and the Manager of the Business Information Systems in the Business Office act as the security administrators for the Accounts Receivable portion of the Banner Student module. The Bursar determines the appropriateness of user access requested and the Manager of the Business Information Systems requests that the access be implemented by the database administrator and maintains and verifies the access granted. The security administrators control access to Banner by assigning authorized users to a user role or roles, or by granting direct access to specific Banner objects (forms, processes, etc.). Each user role has access to a set of forms, reports, and processes within the Banner application. The access granted for most forms, reports, or processes can either be maintenance, which is updating capability, or query, which is view only access.

Users should be granted sufficient access to perform all job duties, but access should be as limited as possible to minimize the possibility of fraud or the exposure of sensitive or confidential information. Restricting access to this information also reduces the risk of the institution violating federal laws or regulations including the Family Education Rights and Privacy Act (FERPA).

## AUDIT OBJECTIVES

The objectives of the audit are as follows:

1. To evaluate the security access granted to Bursar/Cashier's Office users for SunGard Banner Accounts Receivable to:
  - a. determine if access is appropriate for related job responsibilities,
  - b. confirm that employees do not have excessive or conflicting update authority, and
  - c. ensure that proper separation of duties exists.
2. To evaluate the security access granted to non-Bursar/Cashier's Office users of Banner Accounts Receivable to determine the appropriateness of access and any update capabilities.
3. To review the access approval procedures and controls to determine how access is granted, how specific form access needs are determined and approved, and how update form conflicts are resolved.

## AUDIT SCOPE

We examined the following regarding Banner Accounts Receivable Access Security:

- Documentation for the Banner Accounts Receivable system
- Reports from the database administrator for form, report, and process security and for user role security as of June 12, 2008
- User roles for appropriateness of form, report, and process access
- Appropriateness of user role assignments to position and general job duties for all users
- The process by which access is granted to the Banner Accounts Receivable portion of the Student module

## AUDIT SUMMARY

In general, the security setup is strong. The security administrators are conscientious and knowledgeable. Users are assigned to roles that are closely aligned with their functional areas and job duties. With very few exceptions access granted to users is appropriate. Access policies and procedures are in detailed written form with flowcharting.

### Adequate controls and practice exist for the following audit objectives:

- Proper separation of duties
- Access approval procedures and controls

### Opportunities for minor improvement exist for each of the following audit objectives:

- Excessive or conflicting update authority
  - Action Plan Task: Superuser access of AR for Finance superusers will be eliminated.
  - Action Plan Task: Users will be assigned as either a cashier supervisor or a restricted user.
- Access granted to non-Bursar/Cashier's Office users
  - Action Plan: A spreadsheet that is maintained by HR will be utilized to track non-USI AR users and verify continuing organizational affiliation.

### Opportunity for moderate improvement exists for the following audit objective:

- Appropriate access for job related responsibilities
  - Action Plan Task: Request will be made of the Banner DBA to eliminate all but two of the FIN\_AR classes.
  - Action Plan Task: Determine whether to retain remaining FIN\_AR classes and move forward with the elimination of duplicated access.

## CONCLUSION

The completed actions should streamline and simplify maintenance of security access for the Accounts Receivable portion of the Banner Student module.



## Audit Report Federal Grant Compliance

### RESULTS AT A GLANCE

AREAS	RISK MITIGATION			
	Adequate Controls & Practice	Opportunity for Minor Improvement	Opportunity for Moderate Improvement	Opportunity for Significant Improvement
<b>Audit Objectives:</b>				
Compliance with Federal OMB Circular and agency guideline requirements				
Compliance with specific federal grant agreement or contract terms				
Conformance to institutional policies, procedures and guidelines				

### EXECUTIVE SUMMARY

#### BACKGROUND

The Department of Internal Audit has completed an audit of Federal Grant Compliance. Federal grants are subject to a multiple layer set of regulations. The Office of Management and Budget (OMB) issues publications known as circulars which govern grant activity in various economic sectors. Circulars A-21 (Cost Principles for Educational Institutions), A-110 (Uniform Administrative Requirements for Grants and Agreements with Institutions of Higher Education...), and A-133 (Audits of States, Local Governments, and Non-Profit Organizations) apply in whole or in part to colleges and universities. In addition, specific federal granting agencies usually have their own set of requirements, e.g. the Department of Health and Human Services (DHHS) publishes the HHS Grants Policy Statement. In some cases, a specific grant program within an agency will publish its own policy or guidelines. Each individual grant agreement or contract will also contain its own specific allowances and restrictions, e.g. an approved budget.

In each case, the more specific guidelines or policies will govern the grant activities, the allowability of costs, the level of administrative costs recovered, etc. Thus if a budget item is approved by an agency as part of a grant proposal or agreement, but is otherwise generally not allowable per Circular A-21, the approved budget will control the allowability. Similarly, a specific agency or agreement may limit the recovery of Facilities and Administrative (F & A) costs, thus negating the recovery rate negotiated per Circular A-21. The higher level guidance will still control, however, if a more specific publication or agreement does not address an issue. This regulatory structure leads to a complex compliance environment.

#### AUDIT OBJECTIVES

The objectives of the audit are as follows:

1. To verify compliance with federal OMB circular and agency guideline requirements.
2. To verify compliance with the specific federal agency grant agreement or contract terms.
3. To verify conformance with institutional sponsored agreement policies, procedures, and guidelines.

## AUDIT SCOPE

We chose a sample of active or recently closed (as of Fall 2008) federal non-financial aid grant funds for our review. For the detailed examination, the field was narrowed to one grant, "Vanderburgh Correction Nursing 2008." This is the second year (FY 07-08) of a five-year project sponsored by the DHHS. In regard to the chosen project, we examined:

- Grant documentation including proposal and agreement
- Transactional data and supporting documentation
- Applicable OMB circulars and other government agency documentation
- Institutional publications

We also interviewed Business Office personnel to become familiar with internal policies and procedures.

## AUDIT SUMMARY

We found a mix of adequate controls and practices and opportunities for improvement within the stated audit objectives.

### Opportunity for Significant Improvement

We found opportunity for significant improvement in the area of compliance with Federal OMB Circulars and agency guidelines. The major area of concern is time and effort reporting. The classification of 'significant' is based on recent Federal audit findings at other institutions regarding this issue and not their financial materiality. The direct financial impact is small, but federal audit findings tend to raise red flags and result in an expanded audit scope.

### Opportunity for Moderate Improvement

We also found opportunities for improvement in the areas of establishing the allowability of some meal/food costs, indirect cost recovery application, and consistency between practice and internal policies and procedures.

### Adequate Controls and Practice

We found the following areas to have adequate controls and practice:

- Federal cash management
- Budget compliance
- BANNER grant fund classification
- Required financial reporting

Planned actions by audit objective are as follows:

- **Compliance with federal OMB circular and agency guideline requirements**
  - Review current versions of all related federal guidelines to provide framework for effort certification policy revisions.
  - Revise effort certification policy with input from Payroll, Sponsored Research, Internal Auditing, and all departments with active federal grants.
  - To insure allowability of expenditures, include staff accountant in review process for payment requests, credit card transactions, and petty cash transactions.
- **Compliance with the specific federal agency grant agreement or contract terms**
  - Correct all fiscal year 2009 allocations and revise procedure to charge F & A costs as a percentage of actual expenditures.
  - Amend monthly reconciliation of F & A costs to include verification of amounts allocated to departments.
- **Conformance with institutional sponsored agreement policies, procedures, and guidelines**
  - Revise effort certification policy to coincide with current practices.

## CONCLUSION

The completed and planned actions will bring institutional federal grant management into a strong position of compliance and conformance with both federal and institutional requirements.

# Attachment D

## UNIVERSITY OF SOUTHERN INDIANA

### REPORT ON INTERNAL CONTROLS

Internal control refers to the design and use of controls that allow managers to administer current operations, plan for the future, and safeguard an organization's assets. Properly applied, good internal control procedures should insure the efficiency, effectiveness, and economy of any operation. The internal controls over the operational and financial activities of the University of Southern Indiana have been grouped into the following categories:

- **Accounting controls** relate directly to safeguarding assets and the reliability of the financial records. They address authorizations, approvals, and separation of duties between record keeping and asset custody.
- **Information system controls** are concerned with access to systems and data, the integrity of mission critical information, and the physical security of hardware and software systems. They include such controls as user authentication, backup and restore procedures, disaster recovery planning, and protection of equipment against theft and loss.
- **Administrative controls** are concerned with operational efficiency and adherence to policies. They generally include controls such as comparative analyses, performance reports, training programs, and quality control.

The controls identified in this report reflect management's representation of the internal control structure currently in place at the University. The controls in each subcategory are divided into those that conform to best practices and those that deviate from best practices. Deviations from best practices are not necessarily bad practices, but may reflect differences in our environment from that which existed when best practice standards were set. For example, technology has enabled some controls to be built into a process so that a separate step is no longer needed to provide proper control. This is only one form of compensating control. Other compensating controls are identified throughout the report.

#### ACCOUNTING CONTROLS

##### I. ACCOUNTS PAYABLE AND OTHER LIABILITIES

###### A. Conforms to Best Practices

1. Liability control accounts are reconciled with subsidiary records on a regular basis.
2. Accounts payable are maintained independently of cash receipts and disbursement functions.
3. Accounts payable and other liability adjustments are supported by documentation that has been properly reviewed and approved.
4. Procedures exist to facilitate payments to vendors in a timely fashion.
5. Procedures exist to prevent duplicate payments and payments for damaged goods.
6. Procedures exist to ensure proper credit for returned purchases.
7. Debit balances in liability accounts are reviewed regularly and reclassified at year end if appropriate.
8. Year end procedures ensure inclusion of all items purchased during the period.

###### B. Deviates from Best Practices

1. Receiving reports are not required for proof of delivery; therefore, the standard control of a three-way match of vendor invoice, purchase order, and receiving report does not exist prior to payment.
  - a. Compensating controls: Financial managers approve all items ordered via a purchase order. Also see compensating controls below.
  - b. Risk: Minimal. Only small dollar purchases are made outside the purchase order system.
2. Invoices up to \$5,000 are paid by negative confirmation if a purchase order exists and the invoice amount agrees (within reason) with the purchase order amount.
  - a. Compensating controls: Financial managers are notified of invoices scheduled for payment and given 15 days to notify AP of a reason why the vendor should not be paid. If no response is received from the financial manager, or his/her alternate if the financial manager is absent, payment is processed as scheduled.

- b. Risk: Minimal. Financial managers approve all items ordered via a purchase order.

## II. ACCOUNTS RECEIVABLE

### A. Conforms to Best Practices

1. Accounts receivable are maintained independently of cash receipts and disbursement functions.
2. Bad debt write-offs, credit memos, and allowances are approved independently of processing, recording, and collecting.
3. Individual accounts are independently reconciled with the control account on a regular basis.
4. Aged accounts, and accounts with credit balances, are reviewed periodically.
5. Measures exist that encourage prompt collection of student accounts receivable.
6. Procedures exist for follow-up and collection of delinquent accounts.
7. Disputed liabilities are handled by persons other than those receiving payment.
8. Completed invoices are controlled and properly accounted for.
9. Adequate control exists over the mailing of statements to prevent interception prior to mailing.

### B. Deviates from Best Practices

1. Account receivable balances have not been independently confirmed on a periodic basis.
  - a. Compensating controls: None
  - b. Risk: Not yet determined.
2. Only one person can build the billing tables in Banner (the University's enterprise management system), test them, and prepare the student billings each semester.
  - a. Compensating controls: None. A solution is currently being developed.
  - b. Risk: Not yet determined.
3. Follow-up and collection on delinquent receivable accounts not performed on regular or timely basis since conversion to Banner.
  - a. Compensating controls: Banner delinquency codes will help with catch up.
  - b. Risk: Not yet determined.

## III. CASH DISBURSEMENTS

### A. Conforms with Best Practices

1. Check or Electronic Disbursements
  - a. Adequate separation of duties exists between the approval and payment functions.
  - b. All checks are made payable to specific payee.
  - c. Advance signing of checks is impossible because of software security.
  - d. All disbursements are properly authorized and supported by appropriate documentation, which is reviewed before checks are issued.
  - e. All bank accounts and check signatures are properly authorized; check signers are adequately insured.
  - g. Procedures provide for immediate bank notification when an authorized signer of checks changes duties or resigns.
  - h. The supply of blank checks is adequately controlled and secured.
  - i. Voided checks are properly mutilated and held for inspection; old outstanding checks are voided after one year.
  - j. Vouchers, or other approved documentation, are prepared for all expenditures, including wire transfers and Automated Clearing House (ACH) debit entries.
  - k. Facsimile signature is electronically stored in software and applied during check run process.
  - l. A firm procedure establishes the conditions under which disbursements can be made.
  - m. Each bank account is under a separate ledger control.
  - n. Bank accounts are reconciled monthly by a person independent of cash functions.
  - o. The sequence of check numbers are accounted for when reconciling bank accounts.
  - p. The check production system does not omit check sequence numbers during printing or in the event of printing errors.
  - q. A positive pay process is used to verify checks produced to checks processed by the bank for clearing. Exceptions identified by the bank require approval by USI before processing.
  - r. Cancelled checks are returned from the bank electronically which prevents physical alteration after processing.

- s. Bank software requires user ID, a password, and a random number generator provided by the financial institution to approve electronic disbursements.
  - t. Direct deposit files are generated by the Computer Center staff who do not have responsibility in the preparation and disbursement process
2. Petty Cash Disbursements
- a. Petty cash funds are properly authorized, the responsibility of only one person, and are properly safeguarded.
  - b. Petty cash vouchers are signed by the person receiving cash, prepared in ink, and required for each expenditure.
  - c. Petty cash disbursements are supported by original receipts verifying the amount disbursed.
  - d. Reimbursement vouchers to replenish fund are approved by a responsible employee who has no daily cash handling responsibilities.
  - e. Vouchers and attachments are properly cancelled to preclude reuse.
  - f. Petty cash funds are limited to expenditures not exceeding a fixed amount; variances to that amount require special approval.
  - g. Petty cash fund balances are adequate for the activity's needs.
  - h. The funds are verified by surprise counts.
3. Travel Disbursements
- a. The authority for approval of travel requests is established at all organization levels.
  - b. Travelers are educated regarding the institution's travel regulations.
  - c. Travel is supported by an approved travel request form with the exception of local travel within a radius of 50 miles and no overnight stay.
  - d. The business purpose of travel is stated on the face of the travel request.
  - e. Cash travel advances are limited in scope and tightly controlled, and original receipts are required to reconcile travel advances.
  - f. The appropriate financial manager or approved alternate approves all travel reimbursement vouchers.
  - g. All travel vouchers are independently reviewed in detail for allowability and reasonableness.
  - h. Travelers are required to provide original receipts for all travel expenditures, and unauthorized personal travel expenses are excluded from reimbursement.
  - i. Travel plans are made sufficiently in advance to obtain the most favorable transportation rates.
  - j. Procedures are in place to govern student and field trip travel.
- B. Deviates from Best Practices
- 1. Endorsements on cancelled checks are not periodically examined nor are paid checks randomly scrutinized for suspicious and irregular features. The check volume is so large that this would be a daunting task. It is doubtful that such scrutiny would result in identifying an altered or a fraudulently endorsed check.
    - a. Compensating controls: A great number of payments are now being made electronically rather than by paper checks. Check stock has security features which make it difficult to alter. The bank provides 'positive pay' service which catches odd check numbers or mismatched amounts with check number.
    - b. Risk: Minimal.

#### IV. CASH RECEIPTS

- A. Conforms with Best Practices
- 1. Cash receipts are maintained independently of accounts receivable, accounts payable, and check disbursement functions.
  - 2. Cash receipts are promptly recorded using pre-numbered receipts, on-line computer numbered receipts, or cash registers by an individual designated to receive cash.
  - 3. Cash register/cashiering procedures reflect proper daily check-out and documentation.
  - 4. Customer receipts (computer generated or multi-copy hand written) are dated, numerically controlled, and identifiable to a specific cashier.
  - 5. Employees connected with the cash receipts function rotate duties periodically.

6. Cash overages/shortages for each cashier are maintained and recorded on the books.
7. Cash receipts are posted daily to income or subsidiary accounts receivable records.
8. Cashiers are provided separate cash drawers to establish accountability. These drawers are locked during the cashier's absence.
9. Cash receipts are deposited intact on a daily basis; deposits are verified by means of a bank receipt or online access to bank account activity.
10. Adequate facilities are provided for the safeguarding of cash prior to deposit.
11. Safe combinations and keys to cash boxes/files are restricted to an essential number of employees; combinations and locks are changed at each personnel change.
12. Checks returned by the bank are posted to subsidiary accounts receivable records; notification letters are sent to the payor requesting prompt redress.
13. All persons handling cash are adequately insured.
14. All credit card transactions are processed by a third party vendor that meets the payment card industry's data security standards governing cardholder information.

NOTE: The above cash receipts controls apply to the Bursar/Cashier department. They may or may not be in place at all locations that handle cash.

B. Deviates from Best Practices

1. The mail is not opened by someone independent of cashiering or accounts receivable duties. One accounts receivable staff opens the mail daily. This person is also a backup cashier.
  - a. Compensating controls: Mail is opened in a secure and controlled environment and in the presence of other people. A restrictive endorsement is immediately stamped on the check.
  - b. Risk: Minimal.

V. INVESTMENTS

A. Conforms with Best Practices

1. An investment policy has been established by the Board of Trustees.
2. Changes in types of investments in the portfolio are approved in accordance with the investment policy.
3. Investments are purchased and sold only upon proper authorization.
4. Original papers evidencing purchases and sales are properly filed.
5. An independent safekeeping agent is utilized; investments are either in a safe deposit box or in the University vault.
6. Investment documents are under the control of a responsible official as custodian.
7. A record is maintained for each investment, including cost, description, purchase date, maturity date, interest rate, and identifying number.
8. A record of investment income is maintained, and accruals are recorded as investment income is earned.
9. Investments are examined periodically and reconciled to controlling accounts.
10. Earnings are reconciled periodically with published financial records.
11. Confirmations are obtained from outside holders of investment documents.

B. Deviates from Best Practices

1. Procedures do not require that more than one person be present during inspection of investments held in the safe deposit box or the University vault.
  - a. Compensating controls: The bank maintains a record of who visited the safety deposit box on a specific date.
  - b. Risk: Minimal.
2. All persons having access to investments are insured, but the level of coverage may not be adequate if a successful theft should occur.
  - a. Compensating controls: Most investments (CDs, federal paper) are registered in the University's name. If stolen or destroyed, USI would be able to collect. Some government securities are held in the name of the nominee bank and insured by policies of the financial institution or guarantees of the U.S. government.
  - b. Risk: Minimal.

## VI. PURCHASES

### A. Conforms with Best Practices

#### 1. Purchase Order Processes

- a. Purchasing policies are defined by written procedures.
- b. Purchases, other than those from petty cash, by procurement card, or below the minimum dollar threshold, are made on properly approved orders.
- c. The use of confirming (after the fact) purchase orders is documented and monitored.
- d. System approval queues requiring financial manager approval are required to submit purchase requisitions for processing.
- e. Adequate separation of duties exist in connection with issuing approved purchase orders, placing orders with vendors, approving vouchers for payment, processing approved vouchers, and disbursing funds.
- f. Policies provide for the assignment of responsibility for final purchasing decisions at the appropriate level.
- g. All purchase order numbers are system generated and accounted for.
- h. Leasing procedures insure compliance with statutory purchasing regulations, as well as University rules and regulations.
- i. A system of competitive bidding is used.
- j. Long-term contracts are under adequate control.
- k. There is a policy statement with regard to conflicts of interest, including employee-vendor relationships.

#### 2. Procurement Card Processes

- a. All procurement cards policies and procedures have been approved by authorized management.
- b. All cardholders are provided with an up-to-date copy of the policies and procedures, and are required to undergo training before their cards are activated.
- c. All cards are issued in the name of individual employees to fix accountability.
- d. All cardholders are required to sign a cardholder's agreement that states terms and conditions.
- e. New and replacement cards are issued inactive, distributed in a secure manner, and only activated upon action by the cardholder.
- f. Cardholders are held personally responsible for unauthorized or personal purchases, and disciplinary measures are in place for card misuse/abuse.
- g. Card usage is monitored for personal use, and charges are examined monthly for authorization, propriety, and purchasing limits.
- h. Monthly and transactional purchase limits are built into the card system software.
- i. Pre-defined Merchant Category Classification Codes (MCC) are used to eliminate some merchants from card purchases.
- j. A log of card purchases by person and by vendor is retained several months in the online system.
- k. A process exists for reporting and deactivating lost or stolen cards, and liability for fraudulent use is limited between the time of the card being stolen and the time it is reported.
- l. All card purchases are required to be signed-off on by the financial manager of the charged account.
- m. All purchases are required to be supported by original receipts including vendor's name, date of purchase, total amount, itemized description of each item purchased, and business purpose if not evident.
- n. Cardholders are required to reconcile their credit card statement to actual receipts on a monthly basis.
- o. Card usage is monitored for "stringing," i.e., breaking down one large purchase into several smaller purchases to circumvent purchase authorization limits.
- p. There is an established procedure for dealing with disputed transactions with the card issuer.
- q. All cards have expiration dates.
- r. There is a procedure for retrieving the procurement card when an employee leaves the organization.

- B. Deviates from Best Practices
  - 1. Confirming (after the fact) purchase orders that are not initiated by the purchasing department have not been subject to review for best vendor or best price comparisons.
    - a. Compensating controls: Departmental budgets and financial manager authority
    - b. Risk: Unknown.
  - 2. Blanket orders are issued to frequently used vendors for "miscellaneous supplies" so that what is being purchased is not known in advance. If known, some items could be bid out for better prices.
    - a. Compensating controls: Departmental budgets and financial manager authority
    - b. Risk: Unknown.

## VII. PAYROLL

- A. Conform to Best Practices
  - 1. Policies regarding time worked, vacations, sick leave, holidays, and other employee benefits are published in the USI handbook and accessible via the web site.
  - 2. Written approval is required for employee additions and deletions from the payroll, changes in pay rates, and payroll deductions.
  - 3. Time sheets and pay vouchers are approved by someone in authority.
  - 4. There is a segregation of personnel and payroll functions.
  - 5. Procedures exist to ensure that all employees are bona fide, and that employees do not receive more than the authorized salary payment.
  - 6. Payroll checks are either direct deposited to employee's bank or distributed by the Cashier's office.
  - 7. Identification is required before receiving paycheck from the cashier.
  - 8. Procedures exist for the control and disposition of any old, outstanding payroll checks.
  - 9. Payroll office employees are cross-trained on many duties to cover absences.
  - 10. Vacation, sick leave and compensating time off are properly documented and controlled.
  - 11. The payroll bank account is maintained on an imprest basis and reconciled by someone having no payroll duties.
  - 12. Blank payroll checks are adequately controlled and safeguarded.
  - 13. Procedures exist to prevent employees from receiving pay other than through properly approved and processed payroll procedures for services performed.
- B. Deviates from Best Practices
  - 1. No formalized record retention policy has been developed for payroll or personnel source documents.
    - a. Compensating controls: Records are retained for longer than needed rather than being destroyed too soon.
    - b. Risk: Unknown. A retention policy lessens burden to produce records in a legal issue from a period earlier than the period stated in a retention policy.

## VIII. EQUIPMENT AND FIXED ASSETS

- A. Conforms to Best Practices
  - 1. Capital expenditures are authorized by appropriate officials.
  - 2. Equipment acquisitions are originated by requisitions that show description, estimated cost, and accounts to be charged.
  - 3. Equipment additions are controlled by a budget. Variations between budget and actual costs require financial manager approval.
  - 4. A policy exists that differentiates between expenditures to be capitalized and those to be expensed.
  - 5. Identifying information (tag or bar code) is placed on equipment after it is installed or placed in its intended location and removed from equipment prior to disposal.
  - 6. Detailed subsidiary records of equipment are maintained, reconciled to the general ledger by fund, and adjusted when equipment is disposed of or transferred.
  - 7. Physical inventories of all equipment are taken periodically. An inventory of large dollar items is taken at least annually.
  - 8. Inventories are tested periodically by an official having no responsibility for the inventory.
  - 9. A computerized preventive maintenance program is used to schedule and identify inspections and



maintenance for major heating and cooling systems. Other equipment is covered by maintenance agreements with vendors.

10. Equipment is reviewed periodically for the purpose of determining adequate insurance coverage.
11. A procedure exists of identifying and disposing of unused or obsolete equipment. An asset control personnel authorizes the disposal and appropriate paperwork is completed.
12. The sale, transfer, scrapping or dismantling of equipment requires written approval.
13. Surplus equipment sales are publicized, use a computerized anonymous bidding process for purchase, and are reviewed by internal audit.

NOTE: The above policies and procedures apply to equipment under the control of Purchasing & Risk Management and the Physical Plant. Different policies and procedures are in place for the equipment controlled by the Computer Center.

## **INFORMATION SYSTEM CONTROLS**

### **I. DATA OPERATIONS**

#### **A. Conforms to Best Practices**

1. All operations tasks including program and equipment maintenance, computer system upgrades, and testing are scheduled in advance.
2. Operations procedures include recording software and hardware problems, management of the tape/cartridge library, cleaning and performing preventive maintenance on the computer equipment (vendor contract), powering up and shutting down the equipment, and running and correcting jobs.
3. Backups of all systems are performed on a daily basis. Backup procedures include the backup of master files, tables, and transactions; the backup of application programs; the backup of systems software; the backup of automated log data; the labeling and identification of backup files; the retention and timely rotation cycle of backup files; the storage of application, system software, disaster recovery plan, and other system operations documentation at a secure location away from the computer center; system testing of critical backup tapes for readability; cross-training of data processing staff; and removal of backups to a secure off-site storage location.
4. Cross training of staff includes the rotation of operators on each application and operations function and more than one person being familiar with the systems software.
5. A written disaster recovery plan exists which addresses a predetermined priority for application processing, the minimum computer configuration, data and application software, physical facilities, security, etc., necessary for processing critical systems, and personnel responsibilities.
6. All abnormal terminations are logged, and applications have checkpoint and restart procedures which allows processing to continue from the record of the last checkpoint before an abnormal termination occurred.

#### **B. Deviates from Best Practices**

1. Although a written disaster recovery plan exists, it has not been evaluated or updated since 2005,
  - a. Compensating controls: None identified.
  - b. Risk: Not yet determined.

### **II. NETWORK ENVIRONMENT**

#### **A. Conforms to Best Practices**

1. Access by individuals to on-line systems is controlled using passwords and single log-on restrictions.
2. Password controls consist of password change required every 60 days; 6 character minimum length and must be a combination of alpha and numeric characters; password does not appear in clear text during log-on or on reports; password encrypted or password table secured; and lock-out after three unsuccessful log-on attempts. Passwords are assigned to individual users rather than user groups.
3. Security software is in place to detect or prevent unauthorized access to the network environment, and security patches are kept up to date.
4. Network access is terminated when the computer center is notified of employee terminations.

5. All drives and files on the network are scanned for viruses in real time, and virus software is updated as new data is available.
6. There is a firewall protecting the network environment through which all traffic must pass, and all dial-up users must provide authentication to get within the firewall.
7. There are controls in place to prevent denial of service attacks, and to detect intrusion attempts and unusual activity.
8. Access to data is restricted on a "need to know" basis, and physical access to data is restricted.
9. Security logins are required for access to the wireless network and wireless access to the internet.
10. Wireless access points are properly configured to restrict network access, and the network is monitored for unauthorized access points.
11. Security controls are in place to restrict wireless network access through intrusion detection systems, by network segregation, and by requiring users to register for access.

B. Deviates from Best Practices

1. Network administrator passwords do not expire. They are changed on an irregular schedule at least once a year or whenever there are staff changes.
  - a. Compensating controls: Complexity required for network administrator passwords
  - b. Risk: Medium.
2. There is not auto log-off from the network due to inactivity. Some employees remain logged onto the network for extended periods or seldom log off. The workstation is then available for anyone to access in the employee's absence.
  - a. Compensating controls: Other programs accessed from the network do have auto log-off - Banner enterprise management system, 30 minutes; Xtender document imaging system, 20 minutes; and Cognos report writer, 60 minutes.
  - b. Risk: Not yet determined.

### III. PHYSICAL SECURITY

A. Conforms to Best Practices

1. Access to the computer room is limited to operators and other employees whose job duties require physical access to it.
2. Unauthorized access to the computer room is restricted by the use of combination locks.
3. Physical access to the tape/cartridge archives is restricted to the librarian and others only when authorized and accompanied by the librarian.
4. Emergencies can be reported by using an alarm pull box that sounds in the computer room and in the control room in the physical plant.
5. Periodic drills reinforce emergency evacuation procedures.
6. Techniques exist to detect and extinguish fire.
7. Warning sensors exist to alert for water in the computer room and network server area.
8. Backup storage exists in both on-campus (weekly tapes) and off-site locations.

B. Deviates from Best Practices

1. The computer room and network room are located in the lower level of the Orr Center. This area has been subject to water leakage in the past, both from ground water and cooling equipment failure. Flooding from plumbing failures is also a possibility.
  - a. Compensating controls: Work has been done to improve ground water drainage around the building and warning sensors have been installed.
  - b. Risk: Unknown.

### **ADMINISTRATIVE CONTROLS**

I. GENERAL

- a. The University has a statement of mission and objectives.
- b. The University is governed by a Board of Trustees appointed by the Governor of the State of Indiana.
- c. There is a current organizational chart in use which reasonably fixes the responsibility of key personnel.
- d. A formalized internal policy and procedures manual exists and is updated regularly.
- e. The formalized policy includes a code of ethics, a policy on fraud and the reporting thereof, and addresses conflicts of interest.

- f. Written job descriptions exist for all employee positions.
- g. A budgetary control system is in place and monitored regularly.
- h. Financial reports provide complete and timely information.

## II. MANAGEMENT REVIEW

- a. All major channels of communication are utilized effectively.
- b. Fiscal authority has been formally delegated to specific management personnel.
- c. Fiscal responsibility exists at all management levels.
- d. Employees are evaluated regularly.
- e. Managers/supervisors review the evaluations with their employees.
- f. Management provides in-house employee training and educational programs that are job oriented.
- g. Management encourages participation in continuing professional education activities provided by outside organizations.
- h. Management promulgates and upholds ethical practice and behavior in all endeavors on behalf of the University.

### **DISCLAIMER**

No list of internal controls can be all-inclusive, nor can it reveal all the dimensions of any statement regarding internal control. Even though the above list represents the standard operating controls and practices of this university and its employees, there will occasionally be deviations from these controls and practices. Sometimes the deviations are warranted by the circumstances; sometimes by thoughtlessness. To our knowledge, there has not been a willful violation of internal controls that resulted in fraud or personal gain.

**University of Southern Indiana  
Internal Audit Report Summaries  
Calendar Year 2008**

AUDIT NAME				
OBJECTIVE	OBSERVATIONS	RECOMMENDATIONS	MANAGEMENT RESPONSE	STATUS
<p><b>Time Worked vs. Time Reported</b> (1.) Determine the amount of time worked versus the amount of time reported on the official University time sheet.</p>	<p>An unofficial <i>Overtime Tally</i> log was being maintained to track flex time hours for six support staff in the area under review. Two staff redeemed their flex hours within one work week per policy, the remaining staff carried hours across pay periods, but only one person did so regularly and frequently. Time sheets submitted to payroll always reflected a normal work week rather than the actual hours worked.</p>	<p>Review the University policy with support staff and their supervisors, always report actual hours worked to payroll.</p>	<p>Meetings were conducted by the provost and HR director with support staff and supervisors. The policy was reviewed and explained. They emphasized the requirement to report actual time worked on all time sheets from that point forward.</p>	<p>Completed</p>
<p>(2.) Determine if employees have been fairly compensated or granted the appropriate amount of time off.</p>	<p>All six employees had more hours worked than they had been compensated for at the time of the review.</p>	<p>Payroll staff should calculate the number of hours and pay that each employee is entitled to. Give employees option of compensated time off or overtime pay.</p>	<p>Payroll made the recommended calculations. The payroll manager and the HR director met with each person and documented their choice of overtime pay or compensated time off.</p>	<p>Completed</p>
<p>(3.) To evaluate if fraudulent activity occurred.</p>	<p>We found no indications of fraudulent activity. The practice in place was a result of supervisor and administrative misunderstanding of the University's policy on flex time reporting.</p>	<p>None</p>	<p>NA</p>	<p>NA</p>
<p><b>Banner Financial Aid (FA) Security Access</b> (1.) To evaluate the security access granted to Student Financial Assistance staff to:</p>	<p>Generally, users are assigned to roles that are closely aligned with their functional areas and job duties, but some have more access than needed.</p>	<p>Review and scale back role access that was initially granted but now found to be excessive. Schedule time for security maintenance to review user access and its appropriateness.</p>	<p>Agreed with recommendations. Plan to perform periodic reviews of security access every six months after initial review.</p>	<p>In progress: June 2009</p>
<p>a. determine if access is appropriate for related job responsibilities,</p>	<p>Several users had unnecessary update capability for a General Student module form.</p>	<p>Trim user access determined to be excessive.</p>	<p>Access for all FA classes was revised to 'query access only' for the form in question.</p>	<p>Completed</p>
<p>b. confirm that excessive or conflicting update authority does not exist, and</p>	<p>Separation of duties is adequate and numerous compensating controls are in place. Data entry logs are reviewed only when a known problem exists.</p>	<p>Schedule periodic reviews of key field log entries for unusual activity even though a known problem has not been identified.</p>	<p>Periodic reviews will be performed by the Assistant Director on the first day of every month.</p>	<p>Completed and ongoing</p>
<p>c. ensure that proper separation of duties exists.</p>	<p>A few non-departmental staff have inappropriate update capability for certain year-specific forms.</p>	<p>Remove inappropriate update capability.</p>	<p>Inappropriate access was corrected as of 7/21/08.</p>	<p>Completed</p>
<p>(2.) Evaluate security access granted to staff in other departments to determine appropriateness of access and update capabilities.</p>	<p>Two user classes have no members.</p>	<p>Evaluate continuing need.</p>	<p>Null classes will be populated for the automation of federal workstudy payroll entries for FY08-09.</p>	<p>Pending: April 2009</p>

**University of Southern Indiana  
Internal Audit Report Summaries  
Calendar Year 2008**

AUDIT NAME				
OBJECTIVE	OBSERVATIONS	RECOMMENDATIONS	MANAGEMENT RESPONSE	STATUS
(3.) Review access approval procedures and controls.	Access policies and procedures are in place, understood, and followed by the security administrator, but they are not in written form.	Record the access policies and procedures in writing.	Policies and procedures will be documented.	In progress: June 2009
<b>Banner Accounts Receivable (AR) Security Access</b>				
(1.) Evaluate security access granted to Bursar/ Cashier Office staff to  a. determine if access is appropriate for related job duties,	In general users are assigned roles that are closely aligned with their functional areas and job duties. Roles are adequately limited based on needed access for specific tasks or procedures. Some access duplication/fragmentation exists between Banner Finance and AR modules for some users.	Analyze user access and consolidate AR access into AR classes. Eliminate duplicated/fragmented access between Finance and AR.	Agreed with recommendations.	Completed
b. confirm that excessive or conflicting update authority does not exist, and	Excessive or conflicting update capability is not an issue for most users, but there are superusers with extensive update access in both Banner Finance and AR modules.	Evaluate and trim the access of Banner Finance superusers. Adjust AR user's unrestricted charge/ payment posting to correct classification - supervisory or restricted.	Agreed with recommendations.	Completed
c. ensure that proper separation of duties exists.	Separation of duties is enforced by software access restrictions for most. Some duties are separated by policy enforcement with management oversight acting as a detective control.	None	NA	NA
(2.) Evaluate security access granted to staff in other departments to determine appropriateness of access and update capabilities.	Most users external to AR have very limited and query only access. Sodexo (contractor) staff has been granted access to carry out student meal plan functions. USI dependent on Sodexo to notify when users change.	Pro-actively contact areas with non-USI employee users periodically to verify employment and continuing access need.	HR is tracking this information. We are working with them to obtain the needed information.	Completed and ongoing
(3.) Review access approval procedures and controls.	The procedures are documented in detail including flow charting for the approval process.	None	NA	NA
<b>Federal Grant Compliance</b>				
1. Verify compliance with federal OMB circular and agency guideline requirements.	Compliance was strong for many federal requirements, but we found significant opportunity for improvement in time and effort reporting and in establishing allowability for some costs and indirect cost recovery.	Involve relevant departments in devising a process that results in an accurate certification of effort while minimizing payroll reallocations.  Verify that supporting documentation specifically establishes why any generally unallowable expenditure is allowable in each instance.	Proposed a meeting with all relevant persons to work out a solution for the time and effort reporting issue.  A new daily report from Cognos summarizes all requisitions entered against restricted funds. This tool will provide opportunities to communicate with departments to clarify the allowability of purchases before they transpire.	Pending: March/April 2009  Completed and ongoing

**University of Southern Indiana  
Internal Audit Report Summaries  
Calendar Year 2008**

AUDIT NAME				
OBJECTIVE	OBSERVATIONS	RECOMMENDATIONS	MANAGEMENT RESPONSE	STATUS
2. Verify compliance with the specific federal agency grant agreement or contract terms.	Per the grant guidelines, facilities and administrative (F&A) costs were limited to a percentage of direct costs. The F&A rate for this grant was charged on the basis of the approved budget rather than actual costs. This resulted in a higher recovery than should have been taken.	Charge F&A costs as a percentage of actual expenditures, not budgeted amounts.	All grants will be reviewed for compliance, and a new monthly reconciliation of F&A costs will document that all amounts are charged based on the percentage outlined in the agreements.	Completed and ongoing
3. Verify conformance with institutional-sponsored agreement policies, procedures, and guidelines.	Policies and procedures are sufficient; however, there are inconsistencies between practice and internal policies and procedures governing effort reporting.	Revise time and effort reporting policy or alter practice to achieve agreement between policy and practice.	The policy will be amended to reflect current practices.	Pending: June 2009

## **Audit Report Time Worked vs. Time Reported**

### **BACKGROUND**

From an exit conference with a terminating support staff who had been employed in the College of Nursing and Health Profession, the HR director learned that employees in that area may have been instructed to keep two sets of time-keeping records: one of actual hours worked and another that was reported on the time sheets, which were submitted to payroll for processing. This information was shared with the provost, who then met with the dean of the College and the program directors to determine the reliability of the claim. From these meetings it was evident that there was some misunderstanding all around about the distinction between 'flex time' and compensatory time, and the importance of recording actual hours worked on the official University timekeeping document. Internal Audit was brought in to review the past year to determine the level of misreporting.

### **AUDIT OBJECTIVES**

1. To determine the amount of time worked versus the amount of time reported on the official University time sheet.
2. To determine if employees have been fairly compensated or granted the appropriate amount of time off.
3. To evaluate if fraudulent activity occurred.

### **AUDIT SCOPE**

In the course of the review, we analyzed the time reported on an unofficial *Overtime Tally* log maintained by some employees in the College, reviewed correspondence regarding absences and flexible hours worked which was maintained in a centrally located three-ring binder, and reviewed the time reported to payroll for the period beginning January 2007 through the pay period ending March 7, 2008. We also interviewed the dean of the College to obtain her understanding of the practice and the reason for its existence.

### **AUDIT SUMMARY AND OBSERVATIONS**

The practice of logging actual hours worked versus hours turned in on the time sheet began as a means to document flexible work schedules. The *Overtime Tally* log provided a place for the date, an explanation of what occurred, time reported on the time sheet, actual hours worked, columns for plus/minus hours designated as "school requested" or "employee requested", a running balance column, and a column where the supervising program director initialed his/her approval.

The purpose was to allow employees to work flexible hours and to avoid unnecessary overtime. Flex time was attractive because there were times when events or circumstances caused staff to be on duty outside normal working hours, and they could compensate for that by taking time off at other times. The running balance on the log helped each employee to keep track of whether they needed to take time off or work extra. However, on the official time sheet the employee would report a normal work day for each day of the time period, resulting in a full paycheck that otherwise might have been short or might have included overtime.

The University's policy on flexible time is found in the handbook, Item E.8, under Compensatory Time and states

*"An altered work schedule within a given work week should not be confused with reporting compensatory time for use in future work weeks. If an employee works fewer hours on one day to offset longer hours on another day in the same work week, there would be no compensatory time accrued in that work week, as long as the schedule change results in 37.5 (or fewer) hours reported. Such schedule adjustments within a given work week must be approved by the employee's supervisor, and the employee must report actual time worked each day on the timesheet."*

Of the twelve support staff employees in the College of Nursing and Health Professions area, only six employees maintained the *Overtime Tally* log during the time under review. Of those six, two performed their

altered work schedule within a given week most of the time rather than spreading it over a two-week pay period or beyond. Four employees spread their flex time schedule beyond one week or beyond one pay period. And, of these four, only one employee did this on a frequent and regular basis.

We found no evidence that anyone was trying to falsify records. As mentioned above, only half of the employees participated in the plan, and then not in a consistent manner. Participating employees and program directors were operating under the impression that this was an acceptable arrangement based on the direction they had received on how to control overtime hours while still maintaining coverage for vacations, sickness, or special events. The dean accepted responsibility for not paying closer attention to how the documentation was being reported to payroll and for not realizing that the flexible-hours method being practiced by some employees was outside University policy and procedures.

#### **MANAGEMENT CORRECTIVE ACTIONS**

- The provost met with the program directors and explained the inappropriateness and seriousness of the work time reporting processes that were being used by some of the CNHP staff.
- The HR director met with the staff and outlined the University policy on reporting time and explained the differentiation between flex time and comp time.
- The payroll manager calculated the overtime hours and the dollar amount due to each employee who had remaining, unpaid hours from the period under review. Each employee was given the choice to receive compensatory time off or overtime pay.
- The provost met with all the deans, directors, and chairs to review the policy on time reporting and emphasized the need to follow policy at all times.

#### **CONCLUSION**

The corrective actions taken should strengthen controls over time reporting for the College of Nursing and Health Professions as well as all other academic areas.



## Audit Report Banner Financial Aid Security Access

### RESULTS AT A GLANCE

AREAS	RISK MITIGATION			
	Adequate Controls & Practice	Opportunity for Minor Improvement	Opportunity for Moderate Improvement	Opportunity for Significant Improvement
<b>Audit Objectives:</b>				
Appropriate access for related job duties				
Excessive or conflicting update authority				
Proper separation of duties				
Access granted to non-Financial Assistance department users				
Approval process procedures and controls				

### EXECUTIVE SUMMARY

#### BACKGROUND

The Department of Internal Audit has completed an audit of the SunGard Banner Financial Aid system access security. The security maintenance function at USI for the Financial Aid system of the SunGard Banner Student module is separate from security maintenance for the General Student/Admission and Student Accounts Receivable systems. General Student/Admission was covered in a previous audit and Accounts Receivable security access for the Student module will be examined at a later date.

The Assistant Director of Student Financial Assistance acts as the security administrator and data manager for the Financial Aid portion of the Banner Student module. Access requests that originate within the Financial Assistance office are typically sent directly to the Assistant Director. Requests from other departments are normally sent to the Director and forwarded upon approval to the Assistant Director. The security administrator controls access to Banner by assigning authorized users to a user role or roles, or by granting direct access to specific Banner objects (forms, processes, etc.). Each user role has access to a set of forms, reports, and processes within the Banner application. The access granted for most forms, reports, or processes can either be maintenance, which is updating capability, or query, which is view only access.

Users should be granted sufficient access to perform all job duties, but access should be as limited as possible to minimize the possibility of fraud or the exposure of sensitive or confidential information. Restricting access to this information also reduces the risk of the institution violating federal laws or regulations including the Family Education Rights and Privacy Act (FERPA).

## AUDIT OBJECTIVES

The objectives of the audit are as follows:

1. To evaluate the security access granted to Student Financial Assistance employee users for SunGard Banner Financial Aid to:
  - a. determine if access is appropriate for related job responsibilities,
  - b. confirm that employees do not have excessive or conflicting update authority, and
  - c. ensure that proper separation of duties exists.
2. To evaluate the security access granted to non-Student Financial Assistance department users of Banner Financial Aid to determine the appropriateness of access and any update capabilities.
3. To review the access approval procedures and controls to determine how access is granted, how specific form access needs are determined and approved, and how update form conflicts are resolved.

## AUDIT SCOPE

We examined the following regarding Banner Financial Aid access security:

- Security documentation for the Banner Financial Aid system
- Reports from the database administrator for form, report, and process security and for user role security as of January 22, 2008
- User roles for appropriateness of form, report, and process access
- Appropriateness of user role assignments to position and general job duties for all users
- The process by which access is granted to the Banner Financial Aid portion of the Student module
- How the extent of access is determined

## AUDIT SUMMARY

We did not discover any major security issues during our review. Generally, users are assigned to roles that are closely aligned with their functional areas and job duties. Time constraints have prevented a thorough review by the security administrator of the security access granted during the initial go-live of Banner Financial Aid in February 2006.

### Opportunities for minor improvement exist for each of the following audit objectives:

- Appropriate access for job related responsibilities
  - Action Plan Task: Review and reclassify employees' access to reflect appropriate security views.
  - Action Plan Task: Review security access every six months.
- Proper separation of duties
  - Action Plan Task: Review selected key field log entries on the first working day of each month.
- Access granted to non-Student Financial Assistance department users
  - Action Plan Task: Adjust internal audit and computer center classes to remove update capability.
  - Action Plan Task: Populate classes for the automation of FWS wages for the 08/09 award year.
- Access approval procedures and controls
  - Action Plan Task: Record the access policies and procedures in writing.

### Opportunity for moderate improvement exists for the following audit objective:

- Excessive or conflicting update authority
  - Action Plan Task: Revise all FA classes to query only access for form SPAIDEN.

## **CONCLUSION**

The security administrator is very experienced and knowledgeable. She understands the Banner Financial Aid system capabilities and grants appropriate access to users. The completed actions will strengthen controls over access to the Banner Financial Aid system.

## Audit Report Banner Accounts Receivable Security Access

### RESULTS AT A GLANCE

AREAS	RISK MITIGATION			
	Adequate Controls & Practice	Opportunity for Minor Improvement	Opportunity for Moderate Improvement	Opportunity for Significant Improvement
<b>Audit Objectives:</b>				
Appropriate access for related job duties				
Excessive or conflicting update authority				
Proper separation of duties				
Access granted to non-Bursar/Cashier's Office users				
Approval process procedures and controls				

### EXECUTIVE SUMMARY

#### BACKGROUND

The Department of Internal Audit has completed an audit of the SunGard Banner Accounts Receivable system access security. The security maintenance function at USI for the Accounts Receivable system of the SunGard Banner Student module is separate from security maintenance for the General Student/Admission and Student Financial Aid systems. General Student/Admission and Financial Aid access security were covered in previous audits.

The Bursar and the Manager of the Business Information Systems in the Business Office act as the security administrators for the Accounts Receivable portion of the Banner Student module. The Bursar determines the appropriateness of user access requested and the Manager of the Business Information Systems requests that the access be implemented by the database administrator and maintains and verifies the access granted. The security administrators control access to Banner by assigning authorized users to a user role or roles, or by granting direct access to specific Banner objects (forms, processes, etc.). Each user role has access to a set of forms, reports, and processes within the Banner application. The access granted for most forms, reports, or processes can either be maintenance, which is updating capability, or query, which is view only access.

Users should be granted sufficient access to perform all job duties, but access should be as limited as possible to minimize the possibility of fraud or the exposure of sensitive or confidential information. Restricting access to this information also reduces the risk of the institution violating federal laws or regulations including the Family Education Rights and Privacy Act (FERPA).

## AUDIT OBJECTIVES

The objectives of the audit are as follows:

1. To evaluate the security access granted to Bursar/Cashier's Office users for SunGard Banner Accounts Receivable to:
  - a. determine if access is appropriate for related job responsibilities,
  - b. confirm that employees do not have excessive or conflicting update authority, and
  - c. ensure that proper separation of duties exists.
2. To evaluate the security access granted to non-Bursar/Cashier's Office users of Banner Accounts Receivable to determine the appropriateness of access and any update capabilities.
3. To review the access approval procedures and controls to determine how access is granted, how specific form access needs are determined and approved, and how update form conflicts are resolved.

## AUDIT SCOPE

We examined the following regarding Banner Accounts Receivable Access Security:

- Documentation for the Banner Accounts Receivable system
- Reports from the database administrator for form, report, and process security and for user role security as of June 12, 2008
- User roles for appropriateness of form, report, and process access
- Appropriateness of user role assignments to position and general job duties for all users
- The process by which access is granted to the Banner Accounts Receivable portion of the Student module

## AUDIT SUMMARY

In general, the security setup is strong. The security administrators are conscientious and knowledgeable. Users are assigned to roles that are closely aligned with their functional areas and job duties. With very few exceptions access granted to users is appropriate. Access policies and procedures are in detailed written form with flowcharting.

### Adequate controls and practice exist for the following audit objectives:

- Proper separation of duties
- Access approval procedures and controls

### Opportunities for minor improvement exist for each of the following audit objectives:

- Excessive or conflicting update authority
  - Action Plan Task: Superuser access of AR for Finance superusers will be eliminated.
  - Action Plan Task: Users will be assigned as either a cashier supervisor or a restricted user.
- Access granted to non-Bursar/Cashier's Office users
  - Action Plan: A spreadsheet that is maintained by HR will be utilized to track non-USI AR users and verify continuing organizational affiliation.

### Opportunity for moderate improvement exists for the following audit objective:

- Appropriate access for job related responsibilities
  - Action Plan Task: Request will be made of the Banner DBA to eliminate all but two of the FIN\_AR classes.
  - Action Plan Task: Determine whether to retain remaining FIN\_AR classes and move forward with the elimination of duplicated access.

## CONCLUSION

The completed actions should streamline and simplify maintenance of security access for the Accounts Receivable portion of the Banner Student module.

## Audit Report Federal Grant Compliance

### RESULTS AT A GLANCE

AREAS	RISK MITIGATION			
	Adequate Controls & Practice	Opportunity for Minor Improvement	Opportunity for Moderate Improvement	Opportunity for Significant Improvement
<b>Audit Objectives:</b>				
Compliance with Federal OMB Circular and agency guideline requirements				
Compliance with specific federal grant agreement or contract terms				
Conformance to institutional policies, procedures and guidelines				

### EXECUTIVE SUMMARY

#### BACKGROUND

The Department of Internal Audit has completed an audit of Federal Grant Compliance. Federal grants are subject to a multiple layer set of regulations. The Office of Management and Budget (OMB) issues publications known as circulars which govern grant activity in various economic sectors. Circulars A-21 (Cost Principles for Educational Institutions), A-110 (Uniform Administrative Requirements for Grants and Agreements with Institutions of Higher Education...), and A-133 (Audits of States, Local Governments, and Non-Profit Organizations) apply in whole or in part to colleges and universities. In addition, specific federal granting agencies usually have their own set of requirements, e.g. the Department of Health and Human Services (DHHS) publishes the HHS Grants Policy Statement. In some cases, a specific grant program within an agency will publish its own policy or guidelines. Each individual grant agreement or contract will also contain its own specific allowances and restrictions, e.g. an approved budget.

In each case, the more specific guidelines or policies will govern the grant activities, the allowability of costs, the level of administrative costs recovered, etc. Thus if a budget item is approved by an agency as part of a grant proposal or agreement, but is otherwise generally not allowable per Circular A-21, the approved budget will control the allowability. Similarly, a specific agency or agreement may limit the recovery of Facilities and Administrative (F & A) costs, thus negating the recovery rate negotiated per Circular A-21. The higher level guidance will still control, however, if a more specific publication or agreement does not address an issue. This regulatory structure leads to a complex compliance environment.

#### AUDIT OBJECTIVES

The objectives of the audit are as follows:

1. To verify compliance with federal OMB circular and agency guideline requirements.
2. To verify compliance with the specific federal agency grant agreement or contract terms.
3. To verify conformance with institutional sponsored agreement policies, procedures, and guidelines.

## AUDIT SCOPE

We chose a sample of active or recently closed (as of Fall 2008) federal non-financial aid grant funds for our review. For the detailed examination, the field was narrowed to one grant, "Vanderburgh Correction Nursing 2008." This is the second year (FY 07-08) of a five-year project sponsored by the DHHS. In regard to the chosen project, we examined:

- Grant documentation including proposal and agreement
- Transactional data and supporting documentation
- Applicable OMB circulars and other government agency documentation
- Institutional publications

We also interviewed Business Office personnel to become familiar with internal policies and procedures.

## AUDIT SUMMARY

We found a mix of adequate controls and practices and opportunities for improvement within the stated audit objectives.

### Opportunity for Significant Improvement

We found opportunity for significant improvement in the area of compliance with Federal OMB Circulars and agency guidelines. The major area of concern is time and effort reporting. The classification of 'significant' is based on recent Federal audit findings at other institutions regarding this issue and not their financial materiality. The direct financial impact is small, but federal audit findings tend to raise red flags and result in an expanded audit scope.

### Opportunity for Moderate Improvement

We also found opportunities for improvement in the areas of establishing the allowability of some meal/food costs, indirect cost recovery application, and consistency between practice and internal policies and procedures.

### Adequate Controls and Practice

We found the following areas to have adequate controls and practice:

- Federal cash management
- Budget compliance
- BANNER grant fund classification
- Required financial reporting

Planned actions by audit objective are as follows:

- **Compliance with federal OMB circular and agency guideline requirements**
  - Review current versions of all related federal guidelines to provide framework for effort certification policy revisions.
  - Revise effort certification policy with input from Payroll, Sponsored Research, Internal Auditing, and all departments with active federal grants.
  - To insure allowability of expenditures, include staff accountant in review process for payment requests, credit card transactions, and petty cash transactions.
- **Compliance with the specific federal agency grant agreement or contract terms**
  - Correct all fiscal year 2009 allocations and revise procedure to charge F & A costs as a percentage of actual expenditures.
  - Amend monthly reconciliation of F & A costs to include verification of amounts allocated to departments.
- **Conformance with institutional sponsored agreement policies, procedures, and guidelines**
  - Revise effort certification policy to coincide with current practices.

## CONCLUSION

The completed and planned actions will bring institutional federal grant management into a strong position of compliance and conformance with both federal and institutional requirements.

Approval of the proposed 2009 Annual Audit Plan is recommended.

**Attachment E**

**University of Southern Indiana  
Annual Audit Plan  
Calendar Year 2009**

<b>QUARTER BEGINNING</b>	<b>AUDIT AREA</b>	<b>DESCRIPTION</b>	<b>HOURS</b>
January 2009	Bookstore	Cash handling internal control review	8
	Bursar	Cash handling internal control review	10
	Auxiliary enterprises	Physical inventory test count	10
	Purchase Card - 2	Review purchases of randomly selected users	200
	Employee benefit liabilities	Review reconciliation among vendor invoices, the Banner HR system, and Banner Finance	200
April 2009	Eagle Card Office	Operations, financial, and IT review	160
	Accounts receivable	Review and testing of receivable balances	200
	Student Financial Aid	Grants and scholarships	200
July 2009	Financial records	Assist State Board with year end audit and report	200
	Athletics	NCAA Division II compliance review	160
	HR/Payroll	Employee Data Analysis - monitoring fraud indicators using computer assisted audit techniques	160
October 2009	Residence Life	Risk assessment - financial or operational audit	160
	Health Professional Practice Unit	Contract compliance	160
	Non-financial aid grant fund(s)	Compliance with grantor regulations	160

<b>Total Hours</b>	<b>1988</b>
Hours needed	2145
Hours available for unscheduled audits	157