# ACCOUNTS PAYABLE DEPARTMENT
# AUDIT OF SELECTED ACCOUNTING PROCESSES

## THE UNIVERSITY OF NEW MEXICO

**Report 2008-02**
**September 3, 2009**

**Audit Committee Members**

J.E. "Gene" Gallegos, Chair
Carolyn Abeita, Vice Chair
James Koch

**Audit Staff**

G. Christine Chavez, Audit Director
Melissa O'Neill, Senior Auditor
Avedona Lucero, Senior Auditor
Lisa Wauneka, Information Systems Auditor

# CONTENTS

# ABBREVIATIONS

ACH........................Automated Clearing House
Accounts Payable........Accounts Payable Department
CIO........................Chief Information Officer
COBIT......................Control Objectives for Information and Related Technology
DPEZ.......................Direct Pay
EFT........................Electronic Funds Transfer
ERP........................Enterprise Resource Planning
FSM........................Finance Systems Management
FSSC.......................Financial Services Support Center
HR.........................Human Resources
IRS........................Internal Revenue Service
IT.........................Information Technology (formerly ITS)
ITS........................Information Technology Services (now IT)
NSAR.......................Non-Student Accounts Receivable
PO/POs ....................Purchase Order/Purchase Orders
SOPs.......................Standard Operating Procedures
UBP........................University Business Policies and Procedure Manual
University.................The University of New Mexico
UNM........................The University of New Mexico

# EXECUTIVE SUMMARY

As part of the fiscal year 2008 audit plan, the Internal Audit Department conducted an audit of The University of New Mexico (UNM) Accounts Payable Department (Accounts Payable).

The purpose of the audit was to assess the adequacy of Accounts Payable's policies, procedures, and internal controls. Fieldwork included interviews with Accounts Payable personnel, review of processes and procedures, and vouching of selected expenditures. Throughout the audit, Accounts Payable management proactively endeavored to implement recommendations for improving quality control. It appears the Accounts Payable internal controls, policies and procedures are adequate. We identified areas where our recommendations will enhance internal controls, ensure compliance with policies and procedures, and improve security of data. The following summary provides management with an overview of our recommendations.

## POLICIES AND PROCEDURES

The Accounts Payable Manager should ensure that standard operating procedures (SOPs) are written and regularly updated. The Accounts Payable Manager agreed with this recommendation.

## CASH MANAGEMENT INTERNAL CONTROLS

The Accounts Payable Manager should ensure compliance with the University of New Mexico (University) Cash Management policy when tracking accounts receivable. The Vice President for Finance and University Controller should review the policy requiring a second signature on checks greater than $25,000 to determine if this amount is reasonable, or if the dollar amount requiring a second signature should be increased. The Accounts Payable Manager agreed with the recommendation for complying with Cash Management policy when tracking accounts receivable checks. The Vice President for Finance and University Controller reviewed the policy requiring a second signature on checks greater than $25,000, and determined that the current amount is appropriate.

## FINANCE SYSTEMS MANAGEMENT INTERNET NATIVE BANNER ACCESS

Finance Systems Management (FSM) should develop a process to remove the access of transferred and terminated employees, and restrict access for employees performing data uploads. The Associate Controller, FSM, in partnership with the Finance Information Technology (IT) Applications Support team and the Banner Authorizations and Security Committee, will further restrict user access by reviewing and re-developing the security access methodology and approach.

## UNIVERSITY-WIDE INTERNET NATIVE BANNER

The Vice President for Human Resources (HR) should develop a process to segregate employees' duties, by ensuring that employees with the ability to enter employee time into Internet Native Banner cannot also approve the same time - unless compensating controls are developed. The Vice President of HR will ensure HR, Payroll and the IT HR/Payroll Applications Support team

develop a process of compensating controls to monitor employees who both enter and approve time.

The Chief Information Officer (CIO) should ensure a process is developed for on-call employee access removal.  The Enterprise Resource Planning (ERP) Leadership team will develop provisioning and de-provisioning access control permission processes and procedures.

The CIO should ensure approved Internet Native Banner production reporting tools and reports are developed.  The CIO disagrees with the proposed remedy suggested by Internal Audit in the recommendation, but the CIO will determine which applications, tools, and resources are within the purview of the ERP Steering Committee and will work with the ERP Steering Committee to develop standards and strategies regarding future reporting tools and reports.

# INTRODUCTION

## BACKGROUND

The Accounts Payable website states that "The Accounts Payable Department is responsible for all University non-payroll, non-financial aid disbursements. These include payments to vendors, employees, and students using Purchase Orders and Direct Pays."
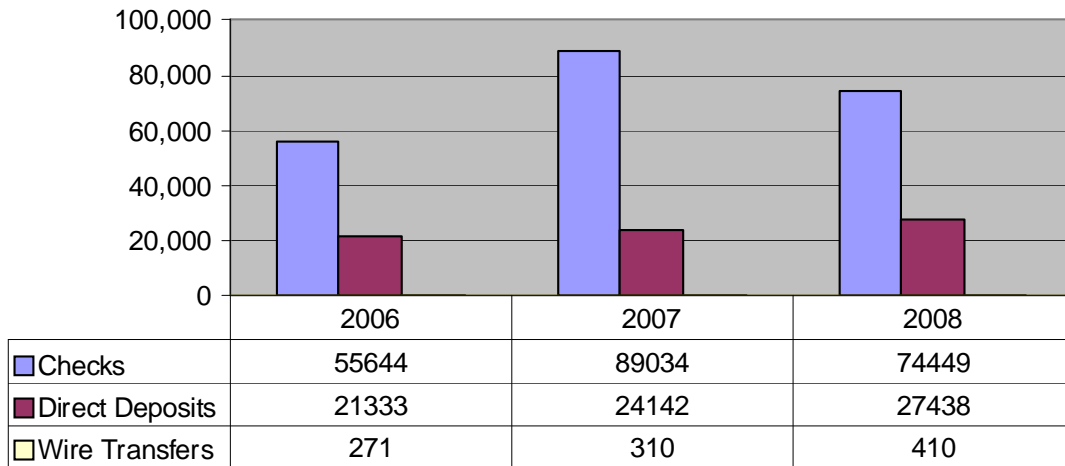
Accounts Payable uses the Internet Native Banner system to process accounts payable transactions. There are two basic disbursement types for which Accounts Payable makes payments: Direct Pays (DPEZ) and Purchase Orders. DPEZs are initiated at the University departmental levels and approved through the necessary accounting office(s). There are two types of Purchase Orders (POs): regular and standing. A regular PO is for goods and a standing PO is for services. The regular PO is designed to pay for a single order of goods, and will be finalized once the order is received and paid.

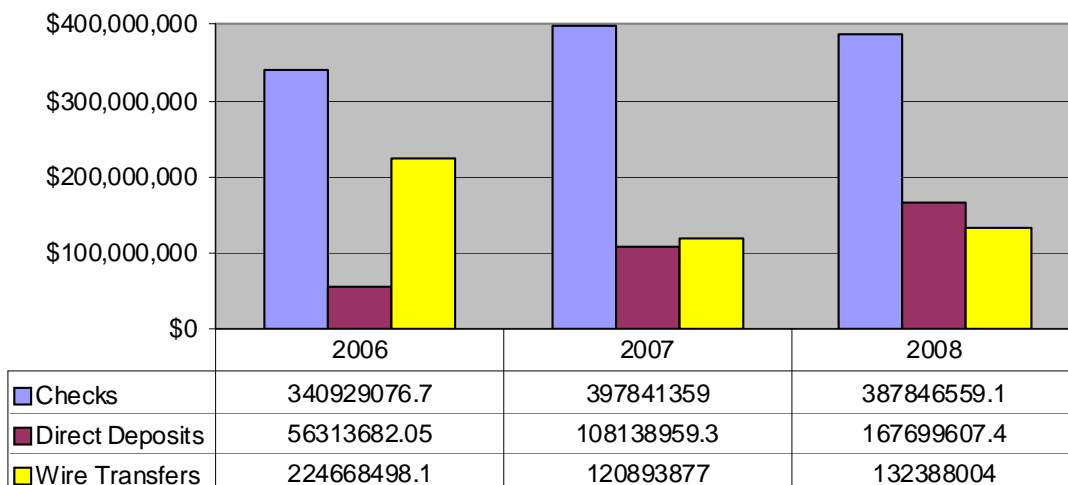Accounts Payable is also responsible for other special processes:

- Foreign Currency/Wire Transfers – These require special handling.
- Electronic Funds Transfer (EFT)/Electronic Payments - With the implementation of Banner, Accounts Payable began making Automated Clearing House (ACH) payments to employees.
- Check Voids/Stop Pays - The majority of checks voided are either due to an incorrect vendor being selected for payment in Banner, or the vendor never receiving the check. The majority of stop payments are due to an incorrect mailing address being selected in Banner.
- Tax Reporting (1099) - UNM must report, annually to the Internal Revenue Service (IRS), payment information for vendors who are 1099 reportable.
- W-2 Reporting – Some direct payments to employees must be reported on the employees' W-2's.
- Credit Memos/External Checks Received – Accounts Payable receives either checks or credit memos from vendors for refunds. The refunded amounts or credit memos are applied to the University department's index where the expense originated.
- Accounts Receivable – Accounts Payable tracks the accounts receivable and money owed to the University that results from Accounts Payable activities such as overpayments to vendors.

Accounts Payable provided the following charts, illustrating the quantity of disbursements by type and the amount of disbursements by type, for Calendar Years 2006-2008:

## Disbursement Quantity by Type

| | 2006 | 2007 | 2008 |
|---|---|---|---|
| ☐ Checks | 55644 | 89034 | 74449 |
| ■ Direct Deposits | 21333 | 24142 | 27438 |
| ☐ Wire Transfers | 271 | 310 | 410 |

## Disbursement Amount by Type

| | 2006 | 2007 | 2008 |
|---|---|---|---|
| ☐ Checks | 340929076.7 | 397841359 | 387846559.1 |
| ■ Direct Deposits | 56313682.05 | 108138959.3 | 167699607.4 |
| ☐ Wire Transfers | 224668498.1 | 120893877 | 132388004 |

## PURPOSE

The purpose of this audit was to review and assess the adequacy of Accounts Payable's policies, procedures, and internal controls to ensure that expenses processed are valid and properly documented, and to test the department's compliance with these procedures and controls.

## SCOPE

Our audit was limited to a review of policies and procedures, selected Banner system security processes, internal controls and financial records for the time period July 1, 2008 through September 30, 2008. A statistical sample of 95 checks was selected for review of the Accounts Payable process. The fieldwork was completed on April 6, 2009.

# OBSERVATIONS, RECOMMENDATIONS AND RESPONSES

## POLICIES AND PROCEDURES

An organization uses policy documents to record their rules and regulations and to identify how they would like their operations managed. Policies are often structured to comply with Federal and State laws. The University has three primary sets of policies: The University of New Mexico Board of Regents' Policy Manual, the University Business Policy and Procedures Manual (UBP), and the University of New Mexico Office of the Secretary Faculty Handbook.

Within the University, there are over 300 separate organizational areas. Each of these areas is responsible for their own operations. Therefore, these areas must develop and maintain the policies necessary to define the rules and regulations specific to their area.

Procedures identify how the policies are to be implemented to ensure compliance with University policies, departmental policies, and Federal and State laws. Written procedures are used to establish what should be done as well as how, when and by whom. The procedures normally identify the step-by-step processes of how to implement and carry out the policy including identifying the specific tasks, and clarifying roles and responsibilities. They should be used to provide consistency in the processes, which can increase overall efficiency. Procedures can also be used to improve communications, establish strong internal controls for regulatory compliance, and standardize bookkeeping to help reduce waste, fraud and abuse.

Well-defined policies and procedures can be used to provide orientation and training for new employees and to refresh the skills of current employees. In addition, they can reduce the risk of confusion, the potential for litigation, and provide documentation for auditors and program reviewers.

Policies and procedures should be widely accessible. This will provide employees with the information needed to effectively make decisions at the most appropriate level, streamline administrative processes, and provide the basis for individual and departmental accountability.

### Policies and Procedures

Accounts Payable has developed some departmental SOPs; however, some of the procedures are not updated, and other procedures are not developed. An example of an undocumented procedure is logging out of the system when leaving computer workstations unattended.

As a result of incomplete operating procedures, the information maintained by Financial Services Support Center (FSSC) documenting the SOPs is not complete and accurate.

In general, policies and procedures help the organization establish and maintain uniformity of operations among employees.  These policies and procedures document how processes are to work, help employees understand how to accomplish their jobs, and assure the information is located in one place for easy reference.

**Recommendation 1**

The Accounts Payable Manager should work with the Accounts Payable staff to ensure that the SOPs are written and regularly updated, and that any changes or updates are reported to FSSC.

**Response from the Accounts Payable Manager**

*We concur with this recommendation.  In June, we began writing new SOPs and updating our existing SOPs.  We expect to have this project completed by 12/31/09.*


# CASH MANAGEMENT INTERNAL CONTROLS

Section 1. "Cash Management" Policy 7200, UBP states that "Faculty, staff, students, and volunteers who receive University monies are responsible for the collection, safekeeping, and deposit of all monies entrusted to them and for the safety of employees who handle the monies. For the purposes of cash management, the term "monies" is defined to include cash, checks, credit card payments, money orders, and other negotiable instruments whether received in person, by mail, or by telephone."

## Accounts Receivable Tracking

Accounts Payable does not channel their accounts receivable through the centralized accounts receivable system at the Bursar's Office.  As a result, there are $3,607 of accounts receivable that have been outstanding prior to June 30, 2005.  Although the amount is not material, appropriate steps need to be taken to resolve these receivables.  In addition, Accounts Payable is not reconciling their accounts receivable ledger to the Banner index for accounts receivable.  This could result in erroneously posted index entries.

Accounts Payable's current procedures for handling accounts receivable do not follow. Section 3.4. "Cash Management" Policy 7200, UBP which states:

> All accounts receivable activity of the University, with the exception of
> University Health Sciences Center patient receivables and Contract and Grant
> receivables, should be channeled through the centralized accounts receivable
> system under the direction of the Bursar's Office. The Bursar's Office is
> responsible for:

- Preparing corrections to customer accounts.
- Posting payments to accounts receivable subsidiary accounts.
- Balancing the accounts receivable trial balances to the general ledger and preparing aging reports.
- Billing and collecting accounts receivable.
- Estimating the percentage of revenue which may be uncollectible.
- Approving the write-off of receivables as uncollectible.

Timely reconciliation of payments is critical to ensure accountability for monies. If some of these duties have been delegated to a department, the Bursar will test and review transactions and processes to ensure internal accountability.

At this point, if Accounts Payable continues to handle their own receivables, they need to get an exception to policy. Section 5. "Cash Management" Policy 7200, UBP states: "Any exceptions to this policy must be approved in writing by the Associate Vice President for Financial Services."

According to the Vice President for Finance and University Controller, "Cash Management" Policy 7200, UBP is outdated and should be revised to include the Non-Student Accounts Receivable (NSAR) Banner module which is specifically for departments to process accounts receivable outside of the Bursar's Office.

**Recommendation 2**

If Accounts Payable continues to handle their own receivables, the Accounts Payable Manager should implement a process that meets the requirements of University policies and procedures.

**Response from the Accounts Payable Manager**

*Due to the unique business nature of Accounts Payable, the Vice President for Finance and University Controller has given us written permission to collect our own receivables from our vendors. This recommendation is resolved as of 8/14/09.*

**Recommendation 3**

The Vice President for Finance and University Controller should work with the Policy Office to update "Cash Management" Policy 7200, UBP for the Non-Student Accounts Receivable Banner module.

**Response from the Vice President for Finance and University Controller**

*We concur with this recommendation. This task has been assigned to the Executive Project Director in Credit, Collections and Merchant Services. Due to limited resources available to us through the UNM Policy office, we don't expect this to be completed prior to 6/30/10.*

## Approval of Large Checks and Wire Transfers

The Chief Finance and Treasury Officer reviews checks equal to or greater than $25,000, signs the signature of the Vice President for Finance and University Controller, and then initials the signature. The Chief Finance and Treasury Officer is authorized to sign on the bank account. In addition, we found that wire transfers or direct deposits are reviewed for release at a lower approval level, thus all payments equal to or greater than $25,000 are not being reviewed and approved at the same approval level. Section 4. "Cash Management" Policy 7200, UBP states that "Cash disbursement equal to or greater than $25,000 requires two signatures from individuals authorized by the bank to sign on the account."

### Recommendation 4

The Vice President for Finance and University Controller should have the Chief Finance and Treasury Officer sign her own name on the checks, since this employee is authorized to sign on the bank account. In addition, the Vice President for Finance and University Controller should set up procedures so that all payments made by the University that are equal to or greater than $25,000 are reviewed and approved at the same approval level.

**Response from the Vice President for Finance and University Controller**

*We concur with this recommendation and have already implemented it, effective August 1, 2009.*

## Review of Policy Requiring Two Signatures on Checks

The policy requiring a second signature on checks has not been reviewed to determine if the $25,000 amount is still reasonable, or if the dollar amount requiring a second signature should be increased. In addition, the current policy does not specifically address wire transfers and direct deposits equal to or greater than $25,000. In order to comply with University policies and procedures, checks equal to or greater than $25,000 must have two signatures. Since the inception of this policy, the number of checks greater than $25,000 disbursed from the University has increased and disbursements are also made by wire transfers and direct deposits.

**Recommendation 5**

The Vice President for Finance and University Controller should determine if the dollar amount of disbursements requiring a second signature is reasonable or should be increased. If the dollar amount should be increased, then the proper steps must be taken through the University of New Mexico Policy Office to ensure that the changes are properly handled in the UBP. Such a change in policy might require approval by The University of New Mexico Board of Regents. In addition, the policy should be updated to address disbursements through wire transfers and direct deposits.

**Response from the Vice President for Finance and University Controller**

*We concur with the recommendation. We have decided that the $25,000 dollar amount for second signatures on checks should remain at $25,000. The dollar threshold is already at an appropriate control level for University transactions. Consequently, no update of policy is necessary. This recommendation is complete as of July 1, 2009.*

## Handling of Returned Checks

Proper internal controls for the handling of checks are not being followed. Returned checks are given to the Accounts Payable employees who are responsible for determining the reason the check was returned. For security and control of returned checks, the original checks should be properly secured, and copies of the checks should be the source document for employees handling these checks. The original checks could be lost or stolen and could possibly be processed for payment.

**Recommendation 6**

The Accounts Payable Manager should develop controls for returned checks.

**Response from the Accounts Payable Manager**

*We concur with the finding and have resolved it, effective August 17, 2009. We now secure all original checks in our department safe. Staff members no longer work directly with original returned checks, but instead with copies.*

# PROCESSING DOCUMENTS FOR PAYMENT

University policy addresses the requirements for paying vendors. Section 1. "Receiving and Paying for Off Campus Purchases" Policy 4370, UBP states:

Proper receiving procedures are critical to the purchasing cycle. The University
will not pay for any purchase of goods or services unless the department certifies
that the goods or services have been received and are satisfactory. Failure to
follow procedures described herein can cause damaged shipments to be accepted
with no recourse, vendor payments to be delayed, and the University's loss of
certain legal rights under the "Uniform Commercial Code" which governs these
transactions. The department receiving the purchase is responsible for following
these procedures when receiving goods or services, processing related damage
claims, returning goods, or requesting payment for goods or services.

To test the process for receiving and paying for off campus purchases, a statistical sample of 95
checks was selected for review for the time period July 1, 2008 through September 30, 2008.

## Review of Documents Processed for Payment

From review of the sample of 95 checks and the supporting documentation, we found some
payments were not processed in a manner compliant with UBP.  Ten (10) out of 51 invoices
were dated prior to processing a PO, and/or purchases were made using either expired POs or
POs that no longer had funds available.

Purchases are initiated by individual departments; therefore, the Purchasing Department is not
always aware of purchases until the department initiates a transaction for payment.

## Recommendation 7

The Purchasing Department should work with departments who process requisitions to ensure
that departmental commitments are not made prior to the issuance of a PO.

## Response from the Chief Procurement Officer

*Some departments will at times receive goods or services prior to a PO being issued.  However,
this isn't always a serious problem or even necessarily an infraction of policy.  The majority of
these transactions fall within the department's delegated purchasing authority of $5,000 based
on PCard rules.  Historically, 97% of these transactions did not exceed the $20,000 bid limits.
Furthermore, we are still generally able to operate within the Procurement rules by applying
existing valid contracts to these invoices.  We will continue to address the serious infractions on
a case-by case basis.*

## Outstanding Credit Memos

For outstanding credit memos, Accounts Payable does not have an aging report and does not
reconcile the index. Without an aging report, it is difficult to properly track how long the
outstanding credit memos have been unresolved. Credit memos are received from vendors for

reasons such as the goods were returned.  Accounts Payable credits the appropriate department's index, but the credit memo amounts are held in an Accounts Payable index until the University does business with the vendor issuing the credit memo or the University requests a refund.  At the time of our review, there was $15,223.86 in outstanding credit memos that had not been resolved.

**Recommendation 8**

The Accounts Payable Manager should work with the staff to develop an aging report, address the status of the outstanding credit memos and reconcile the index.

**Response from the Accounts Payable Manager**

*We concur with the finding and have resolved it effective July 1, 2009.  Accounts Payable now runs a monthly open credit memo report and uses it to reconcile the open items.  We now regularly request refunds from vendors for unapplied credit memos.  We also remove credits that have been proven to be refunded or have been applied to other invoices.*

# EMERGENCY DEPARTMENTAL PLAN

## <u>Emergency Accounts Payable Plan</u>

An Emergency Accounts Payable Plan was developed; however, it is unclear what type of emergency the plan is addressing.  Therefore, employees may not know when to execute the plan.  In order for the plan to be of any value, it should define what constitutes an emergency.

**Recommendation 9**

The Accounts Payable Manager should include information defining what constitutes an emergency in the Emergency Accounts Payable Plan, and should test the reliability of this plan.

**Response from the Accounts Payable Manager**

*We concur with the recommendation and have resolved it effective 6/30/09.  Accounts Payable worked with ITS on a Business Impact report which evaluated acceptable risks and losses.*

# PLANS TO IMPROVE EFFICIENCY

Accounts Payable has a goal to increase efficiency by developing a plan to scan and shred documents.  Accounts Payable is also evaluating ways to more efficiently process UNM General

Library acquisitions. The Chief Procurement Officer is in support of Accounts Payable's continued pursuit to improve efficiency in the following areas.

## Scanned and Shredded Documents

To increase the efficiency of handling documents at Accounts Payable, they are currently scanning documents. However, they are not yet shredding these scanned documents because a destruction plan must be developed and approved by the New Mexico Commission of Public Records State Records Center and Archives before documents can be shredded.

During the course of this audit, there were some instances where the scanned documents were incomplete or illegible. The scanned documents are not the official record because the destruction plan has not been approved. Therefore, at this time it is not a significant issue. However, once a plan is developed and approved, the quality control process should be reviewed to ensure that the scanned documents are complete and legible before they are shredded.

The objective of scanning and shredding documents is to eliminate the need for filing and maintaining hard copies. The scanned documents become the official copy of record. A quality control step assures that scanned documents are reviewed for completeness and readability before they are shredded, and it also ensures compliance with the University of New Mexico Retention Schedule. There may be some departments that are required to maintain the original documents such as Contract and Grant, Main.

### Recommendation 10

The Accounts Payable Manager should continue to work towards the goal of shredding documents. The Accounts Payable Manager should also work with the Associate Director of University Services to obtain approval from the New Mexico Commission of Public Records State Records Center and Archives for the destruction of scanned documents. Following this approval, a written records destruction procedure should be implemented. In addition, the Accounts Payable Manager should work with the Manager of Contract and Grant, Main, to determine if original documentation must be maintained for certain contracts or grants.

### Response from the Accounts Payable Manager

*Accounts Payable has been working in conjunction with other Financial Services departments as well as ITS on this major initiative for quite some time. This massive project requires significant resources, research, planning and documentation. Due to recent UNM budget cuts and the limited resources available to us, we cannot commit to a timetable at this time. We will instead work with Financial Services and ITS to prioritize this project with all other priority projects.*

### Recommendation 11

Once the process in Recommendation 10 is developed, the Accounts Payable Manager should review the quality control process to assure that scanned documents are legible and complete, to be compliant with the New Mexico Commission of Public Records State Records Center and Archives.

### Response from the Accounts Payable Manager

*We concur with the recommendation. We had already planned on developing a quality control process to complement the imaging operation and will do so at the appropriate time. However, the timeline is contingent on the State approval of the imaging plan in recommendation 10 (above) so we cannot commit to a timetable at this time.*

### <u>General Library Payments</u>

Accounts Payable would like to improve the purchasing process for the Acquisitions Department at the UNM General Library, because the current process appears to be inefficient. The current process requires:

- An employee at the Library processing the DPEZ;
- An employee in Unrestricted Accounting reviewing and processing the paper document; and
- Employees in Accounts Payable scanning, and filing the documents.

Accounts Payable is evaluating ways to improve efficiency when processing UNM General Library acquisitions. Depending on the process developed, controls should be in place to ensure that supporting documentation is properly maintained.

### Recommendation 12

In an effort to improve the process, the Accounts Payable Manager should continue to work with FSM to develop a more efficient process for purchasing of acquisitions at the UNM General Library. If the purchasing documents are maintained outside of Accounts Payable, then Accounts Payable should work with the Library to implement controls to ensure that documents are properly maintained.

### Response from the Accounts Payable Manager

*Accounts Payable has been working in cooperation with other Financial Services departments as well as ITS on this project since long before this audit. Due to recent UNM budget cuts and the limited resources available to us, we cannot commit to a timetable at this time. We will instead*

*work with Financial Services and ITS to prioritize this project with all other priority projects. It should also be noted that there is no finding here, no infraction. Instead, this is just a recommendation to enhance an otherwise functioning business process for another department.*

# OTHER ISSUES

## Vendor Maintenance Files

One employee in Accounts Payable who processes 1099s also has access to the Vendor Maintenance Files. The Vendor Maintenance Files list the vendors that have been approved by the University, and only the Purchasing Department should have access to this file.

For proper controls and segregation of duties, employees within Accounts Payable should not have access to or the ability to change information in the Vendor Maintenance Files. The Purchasing Department should control the Vendor Maintenance Files. Both departments feel that the employee processing the 1099s should have access to the Vendor Maintenance Files to be able to efficiently perform the duty. This process does not follow proper segregation of duties.

## Recommendation 13

If this employee continues to have access, the Chief Procurement Officer should establish compensating controls whereby both departments verify the changes made by the Accounts Payable employee are appropriate.

## Response from the Chief Procurement Officer

*We concur with this recommendation. We are currently working with Finance Systems Management to have this issue resolved. We expect this to be completed by 9/30/09.*

## W-2 Processing

An automated file for W-2 processing that Accounts Payable submits to the Payroll Department is not secure. The data in the file can be altered after it is submitted, and it can be submitted more than once. A new automated system was developed to submit W-2 information to Payroll from Accounts Payable. At the time of the audit, this process was in the early stages of implementation, therefore some of the concerns had not been addressed.

After the file is submitted electronically to Payroll, it should be secured to prevent changes to the data, and there should be a process to prevent the file from being resubmitted. Without controlling this data, issues could result regarding improper reporting of W-2 information.

**Recommendation 14**

The Accounts Payable Manager should work with FSM, who designed this feed, and with the Manager of Payroll to fix the process so that the information in the file can not be manipulated at either Accounts Payable or Payroll, and the file cannot be submitted twice.

**Response from the Accounts Payable Manager**

*We appreciate the recommendation, but cannot comply due to recent budget cuts and the limited resources available to us. We will instead use other compensating controls (Hash Totals) to tie out the file on both the Accounts Payable and Payroll sides. We expect to have an improved process in place by 11/30/09.*

**UNM Foundation**

Accounts Payable is processing salary payments for non-UNM employees who work for the UNM Foundation. A DPEZ is processed at the UNM Foundation through Paychex, Inc. This DPEZ is then processed for payment at Accounts Payable. Good business practices and proper segregation of non-UNM functions require the UNM Foundation have their own banking system to process their employees' payroll. The UNM Foundation has not set up a banking function to pay their employees, and therefore the University is responsible for payment of non-UNM employees.

**Recommendation 15**

The Vice President for Finance and University Controller should continue to work with the President of the UNM Foundation to ensure that the UNM Foundation sets up their own banking function so that Accounts Payable is not responsible for the payment of non-UNM employees.

**Response from the Vice President for Finance and University Controller**

*We concur with this recommendation and we will continue to work with the UNM Foundation. We expect to have this fully implemented by June 30, 2010.*


## FSM INTERNET NATIVE BANNER PROCESSES

FSM has developed procedures and processes to manage Internet Native Banner security, but due to resource constraints during implementation, the Internet Native Banner security that was developed needs to be enhanced to further ensure that the appropriate infrastructure, policies, procedures, and standards are in place. A review of Accounts Payable employees' Banner access identified the following issues.

## Access of Terminated and Transferred Employees

Currently, FSM user account management processes do not verify that terminated, transferred and on-call employees' Internet Native Banner user accounts are locked, and that all access is removed. Control Objectives for Information and Related Technology (COBIT) DS5.4 Ensure Systems Security User Account Management best practices recommendation states:

> Management should establish procedures to ensure timely action relating to requesting, establishing, issuing, suspending and closing of user accounts.

Users should only have the access required to perform their specific job duties. Additional access may result in unauthorized use, unintentional modification, disclosure, damage, or loss of the information system or information system data.

## Recommendation 16

The Associate Controller for Finance Systems Management should develop a process that requires:

- The user accounts of terminated employees are locked, and the account passwords are changed; and
- Users transferring to other departments within the University have their previous access removed upon completion of the transfer. The employee's new supervisor should approve new access requests.

## Response from the Associate Controller, Finance Systems Management

*Internet Native Banner security administration is not solely a function of Finance Systems Management, but rather a shared responsibility of the overall Enterprise Resource Planning (ERP), managed and overseen by the Banner Authorizations and Security Committee. This committee is comprised of representatives from Finance, Human Resources, Payroll, Shared Components, Student and the Office of Information Assurance. As such, this committee has been tasked with developing automated processes for locking of user accounts for terminated employees as well as with removal of users' access for organization changes as part of the De-provisioning project. Until this project is complete, the Banner Authorization and Security Committee has implemented manual procedures for locking terminated user accounts as well as developing a report of employees who have changed organizations for manual review and determining appropriate action to be taken on access. This recommendation was addressed in a previous response to an internal audit recommendation related to the ITS Security Audit over a year ago.*

## Direct Table Access for Data Uploads

Accounts Payable and other employees were granted access to certain Internet Native Banner functions in a less than optimal manner. Accounts Payable and other employees have default Oracle roles that allow direct table access into production data for querying and modifying table data during data uploads.

According to Oracle Security Step by Step, access to table data should be properly secured in accordance with best practices.

> Oracle Access Controls Action 3.8.10 states: "Create roles to control access to the underlying data through packages, not directly granting access to tables. Then grant the roles to the relevant business users."

Additional user access may result in unauthorized use, unintentional modification, disclosure, damage, or loss of the information system or information system data.

## Recommendation 17

The Associate Controller for Finance Systems Management should restrict query and modify access to production table data by:

- Assigning a select number of Finance users the ability to upload data into Banner; and
- Using the Internet Native Banner upload process for processing of uploaded transactions.

## Response from the Associate Controller, Finance Systems Management

*Currently only a select number of Finance users have been granted security access to upload data into Banner. This access is administered through an Oracle role that is tied to specific Banner core office roles only. The methodology for granting security access was an approach developed at the time of the Finance implementation in 2004. Finance Systems Management (FSM) in partnership with the Finance IT Applications Support team and the Banner Authorizations and Security Committee, who have oversight of Oracle roles, will review and re-develop this security access methodology and approach as well as review, refine and restrict access to an even more restrictive population of users. Given there is currently a workable process in place, existing limited resources and other competing priorities (Banner 8 upgrade), this effort will take place in 4th quarter of 2010, after the Banner 8 upgrade and other competing priority projects have been completed.*

# UNIVERSITY-WIDE INTERNET NATIVE BANNER PROCESSES

The University has developed processes to manage Banner security, but due to resource constraints during implementation, the Internet Native Banner security that was developed needs to be enhanced to further ensure that the appropriate infrastructure, policies, procedures, and standards are in place.  Issues that affect all Internet Native Banner users were found in the audit of the Accounts Payable department.  These issues should be addressed and resolved by management representatives from all areas using Internet Native Banner.

## Payroll Timekeeping Segregation of Duties

Internet Native Banner payroll time keeper (data entry for timesheet submission) and time approver permissions are sometimes given to the same employee.  Employees have permissions for both of these functions, giving these employees the ability to enter <u>and</u> approve time.  This was allowed so small departments with few employees can meet payroll processing deadlines.  Employees will not get paid unless time is entered and approved.

Payroll time entry and payroll approver duties should be segregated.  Adequate internal controls require that no one employee be allowed to initiate and approve the same transaction.  By combining these duties, employees may have the ability to modify their paychecks by reporting unearned overtime or under reporting sick and annual leave.  In addition, timesheet errors may not be identified without a secondary review.

## Recommendation 18

Human Resources should not allow one user to have both the Payroll Time Keeper and Time Approver roles unless compensating controls are developed.  Compensating controls may include:

- Identification of employees with both roles, and implementation of a solution where the employees cannot both input and approve the same timesheet; and
- Developing monitoring reports for management review of time that is input and approved by the same employee.

## Response from the Vice President of Human Resources

*We concur.  It is inappropriate for one employee to both enter and approve the same time sheet in the Banner HR/Payroll System; however, we also recognize the need for a single employee to have access to both roles so that he/she has the capability to serve as either the timekeeper or the time approver for individual transactions.  This is essential to ensuring that there is appropriate primary and backup support to pay employees.  The following compensating controls are already in existence:*

1. *Per UBP 2610, Time and Leave Reporting, a hard copy time sheet, signed by the employee and the employee's supervisor, is required to be completed for every nonexempt staff and student employee for each biweekly payroll. The authorized administrator serving as the time approver in the Banner HR/Payroll system is required to conduct a full reconciliation of internal time sheets to the electronic report as soon as possible but no later than the next scheduled payroll deadline. The department is required to maintain both the time sheets and the reconciliation for a period of four years or in accordance with grant requirements, whichever is greater. An exception report is available to assist in the collection of annual and sick leave for exempt employees.*

2. *Both the timekeeper and the time approver are required to complete training prior to being granted the access to perform time entry functions in the Banner HR/Payroll system. This training emphasizes that, procedurally, one employee should not serve as both the timekeeper and the time approver on the same transaction. The training guide explicitly states, "For internal control purposes a timekeeper may not assume the role of timekeeper and approver in the same period."*

3. *The Banner HR/Payroll system tracks both the person entering time and the person approving time for every time entry transaction, providing a clear audit trail to assist in the review of transactions.*

4. *The Time Entry Status Report (PZRTNOT), available to management, identifies the individual that input time for each employee as well as the primary approver for the department.*

*To strengthen these compensating controls, the Division of Human Resources will work in collaboration with Payroll and the IT HR/Payroll Applications Support Team to:*

1. *Finalize the report that has been developed to identify when the timekeeper and time approver are the same for an individual transaction by 12/31/2009.*

2. *Develop a process for regular monitoring of the report and any necessary escalation of communications to the appropriate levels at UNM by 3/31/2010.*

3. *Review other options for capturing and approving time in the Banner HR/Payroll system, such as Web Time Entry, that will eliminate or minimize the possibility of an individual both entering and approving time on the same transaction. Make a recommendation on the approach by 6/30/2010.*

## Access of On-Call Employees

ERP has not developed a process to ensure departments are removing on-call user access in a timely manner. Currently, ERP user account management processes do not verify that on-call

employees' Internet Native Banner user accounts are locked, and that all access is removed upon completion of the on-call assignment.  Control Objectives for Information and related COBIT DS5.4 Ensure Systems Security User Account Management best practices recommendation states:

> Management should establish procedures to ensure timely action relating to requesting, establishing, issuing, suspending and closing of user accounts.

Users should only have the access required to perform their specific job duties.  Additional access may result in unauthorized use, unintentional modification, disclosure, damage, or loss of the information system or information system data.

## Recommendation 19

The Chief Information Officer, whose function is to facilitate and coordinate decisions related to ERP policy, process and investment, should ensure a process is developed to remove on-call employees' access to Internet Native Banner that includes:

- Termination of on-call employees' access when they have not worked in a specific period of time; and
- Locking and unlocking users' accounts as necessary for on-call employees who work sporadically.

## Response from the Chief Information Officer

*Agree.*

*The ERP Leadership team, via a "Provisioning/De-provisioning" subcommittee, has been tasked with developing provisioning/de-provisioning and access control permission processes and procedures.*

*This finding will be presented to the ERP Leadership and Steering Committees (and possibly to the "Provisioning/De-provisioning" subcommittee) for disposition, approval, funding and/or prioritization.  Based on these committees' analysis and decisions, more specific strategies and dates on how best to address this issue will be possible.*

*Expected date of ERP Leadership's prioritization and scheduling decision: end of October 2009.*

## Direct Table Access by Users

FSM has developed reporting methodology for obtaining reports from Internet Native Banner production, but University-wide procedures for reporting have not been developed.  Employees hold multiple Oracle default roles that allow direct table access into production data for querying table data for reporting purposes.

According to <u>Oracle Security Step by Step</u>, access to table data should be properly secured in accordance with best practices.

> Application Development Action 7.8. states: "(Oracle) Ad-hoc queries should be disallowed against production database.  Access should be restricted to correct applications, approved reporting tools and DBA access."

Users running long, ad-hoc queries may cause a denial of service and a performance decrease in production.

## Recommendation 20

The Chief Information Officer, whose function is to facilitate and coordinate decisions related to ERP policy, process and investment, should ensure access to Internet Native Banner production is restricted to correct applications and approved reporting tools.  This can be accomplished by developing approved reporting tools and reports, limiting reporting from Internet Native Banner production to only those queries that cannot be obtained from the Operational Data Store, and restricting ad-hoc queries in the production database.

## Response from the Chief Information Officer

*Disagree.  The Recommendation 20 implies a specific remedy.*

*The CIO is currently leading the effort to establish a baseline for the University's ERP system, Banner, which will further clarify what applications, tools and resources are within the purview of the ERP Leadership and Steering Committees.  The initial baseline review is expected to complete January 2010.*

*The CIO will then work with the ERP Leadership and Steering Committees to reach a consensus (and/or develop standards and strategies) concerning the use of reporting tools and reports. Due to the significant funding reductions required by Information Technologies over the last 9 months, the Office of the CIO will be required to evaluate the current reporting / tools environment with an emphasis on data warehousing.*

*Once the initial baselining initiative is complete, the task of reviewing current applications, reporting tools and approaches and then developing standards and strategies regarding future reporting tools and reports will be placed into the IT portfolio and prioritization process and then be presented to the ERP governance Committees for their disposition, approval, funding and/or prioritization.  Based on their analysis and decisions, more specific dates will be possible.*
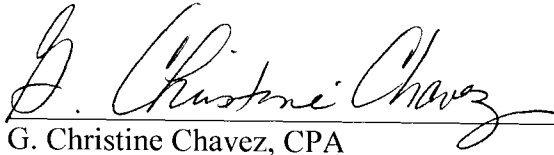
# CONCLUSION

It appears that Accounts Payable is operating as planned. However, opportunities to strengthen internal controls were identified in the Accounts Payable Department and in departments initiating purchases. Meetings with staff in the Accounts Payable Department resulted in indications that implementation of the recommendations made in this report will further strengthen internal controls when processing accounts payable.

For Internet Native Banner issues:

- User access should be properly secured;
- Approved production reporting tools and reports should be developed; and
- Procedures should be developed to address University-wide Internet Native Banner internal control and security issues.

# APPROVALS

_(signature)_

G. Christine Chavez, CPA
Director, Internal Audit Department

Approved for Publication

_(signature)_

Chair/Audit Committee