AGENDA

THE UNIVERSITY OF WEST FLORIDA
BOARD OF TRUSTEES

Audit & Operations Committee Meeting
August 5, 2015 - 9:30 a.m.

University of West Florida Alumni Room, Bldg. 12
11000 University Parkway, Pensacola, FL 32514

Call to Order/Roll Call. . .. . Susan O'Connor, Chair

Greeting. . . . . Susan O'Connor

Action Item(s):

1. Acceptance of Internal Auditing PCard Audit Reports 4th Quarter 2014-2015
2. Acceptance of Internal Auditing Reports: Vendor Master File-14/15-006 and Lab Safety & Security-15/16-001
3. Approval of BOT 13.01-09/15 Identity Theft Prevention Policy
4. Acceptance of Revised UWF Human Resources Policy HR-20.02-07/15 Recruitment, Selection and Appointment

Information Item(s):

1. Internal Auditing Update on Activities

Other Committee Business:

Adjournment

Action Item

UWF Board of Trustees Meeting
Audit & Operations Committee
August 5, 2015

Issue: Internal Auditing PCard Audit Reports ~ Results for Quarter 4 and the Annual Update (July 2014-June 2015)

Proposed action: Acceptance

Purpose

To provide UWF Senior leadership a short, clear overview of the PCard audits completed during the quarter and highlight results. Our main objective is to report the status of PCard audits and any issues or findings requiring action.

Background

Internal Auditing has been charged with auditing PCard holder and approver activity as well as departmental activities and internal controls. The objectives of these audits were to determine if departments complied with UWF PCard policies and procedures, as well as to evaluate the level of understanding of PCard policies among PCard holders and approvers. UWF presently has 425 PCard holders distributed across 118 departments. For the 2014/15 fiscal year $12,916,277 in expenses were paid via PCard at UWF to 3,967 vendors.

Notable Strengths

The approvers are consistently signing transaction documentation, and there were no findings involving missing documentation. Internal Control processes such as Card and Card numbers are being kept secure, and passwords have remained confidential and accessible only to the approved. Files are orderly and staff seemed to be well-trained.

Results for Quarter 4 (April-June 2015)

Five departments[1] encompassing 27 cardholders were examined on a sample basis. Individual reports were distributed to department heads and Procurement and Contracts upon completion of the audits. The totals below show the volume of activity occurring for these 5 departments and the amount tested. All reports are available from Internal Auditing.

Number of Departments Reviewed	Number of Cardholders	Number of Transactions Occurring	Number of Transactions Tested	Total PCard Expenditures of Depts.	Total PCard Transactions Tested
5	26	1039	262	$416,017	$222,292

Audit Opinion for the PCard Audit				
EXCELLENT	**GOOD**	**FAIR**	**POOR**	**Total**
4	**1**	**0**	**0**	**5**

[1] Departments audited (listed by audit opinion): ***Excellent*** – Counseling and Psychological Services, Marketing and Communications, University Advancement, and Career Services; ***Good*** – Recreation and Sport Services; ***Fair*** – None; ***Poor*** – None.

Most Common Findings for Quarter 4 (April-June 2014)

1. The JP Morgan bank statements were not reviewed during the reconciliation process, or were not kept on file.
2. In one department, transactions were allowed to Autopost.

Results-Fiscal Year 2014/15

This is a summary of the PCard audit results for Fiscal Year 2014/15. Thirty-two departments[2] encompassing 160 cardholders were examined on a sample basis. Individual reports were distributed to department heads and Procurement and Contracts upon completion of the audits. The totals below show the volume of activity occurring for these 32 departments and the amount tested. All reports are available from Internal Auditing.

Number of Departments Reviewed	Number of Cardholders	Number of Transactions Occurring	Number of Transactions Tested	Total PCard Expenditures of Depts.	Total PCard Transactions Tested
32	160	6,034	1,419	$ 2,226,309	$ 1,119,922 (50%)

Audit Opinion for the PCard Audit				
Excellent	**Good**	**Fair**	**Poor**	**Total**
15	**11**	**5**	**1**	**32**

MOST COMMON FINDINGS IN THE FISCAL YEAR

1. The JP Morgan bank statement was not reviewed during the reconciliation process.
2. The business purpose was unclear on the PCard documentation.
3. Sales tax was paid and a refund was not requested.
4. Cardholder did not sign transaction documentation.

Recommendation: Acceptance of the Internal Auditing PCard Reports for the Quarter and Fiscal Year Summary of PCard Audits for FY 2014/15.

Implementation: For PCard audit reports issued during the third quarter (April-June 2015), management will implement corrective actions to be completed in the first two months of fiscal year 2015/16. Internal Auditing will follow up to determine if adequate corrective actions occurred.

Fiscal Implications: Fiscal oversight by the UWF Board of Trustees.

Prepared by: Cindy Talbert, Interim Internal Audit Director, 474-2638, ctalbert@uwf.edu
Presenter: Cindy Talbert, Interim Internal Audit Director

[2] Departments audited (listed by Audit Opinion): ***Excellent***: Psychology, Management and MIS, College of Business Dean's Office, Anthropology, Educational Research Center for Child Development, Marketing and Economics, Registrar, Accounting and Finance, Office of International Education and Programs, Facilities Development and Operations, Social Work, University Advancement, Counseling and Psychological Services, Marketing and Communications, Career Services; ***Good***: FPAN, Financial Aid, Math and Statistics, Teacher Education and Educational Leadership, Electrical and Computer Engineering, Office of Equity, Diversity, and International Affairs, 21st Century Scholars, Intercollegiate Athletics, Government, Exercise Science and Community Health, Recreation and Sports Services; ***Fair***: Archaeology Institute, Music, Theatre, Computer Science, Research and Sponsored Programs; ***Poor***: Communication Arts.

Action Item

UWF Board of Trustees Meeting
Audit and Operations Committee
August 5, 2015

Issue: UWF Internal Auditing & Management Consulting-Internal Auditing Reports Issued

Proposed action: Acceptance

Background information:
Internal Auditing & Management Consulting (IAMC) completed 2 audits during the period May-July 31, 2015: Vendor Master File and Lab Safety and Security, which were part of the 2014/15 audit plan. Below are synopses of each with full reports as an attachment to this agenda item.

I. Vendor Master File-14/15-006

The primary objectives were to evaluate controls over new vendors added to the file, to assess compliance, to determine whether payments were made only to authorized vendors. Audit fieldwork began on January 13, 2015, and ended on May 15, 2015. The audit report was issued June 29, 2015.

Results:
The audit report included 4 findings, as follow (*expected implementation dates are in parentheses*):

1. Procurement and Contracts should develop a standard operating procedure for annually deactivating any vendor that has not been used in the previous 5 years. (*December 15, 2015*)
2. Procurement and Contracts should take additional steps to identify potential duplicate vendors in the Vendor Master File, on a periodic basis. (*December 15, 2015*)
3. Procurement and Contracts should make specific enhancements to their background review of new vendors. (*December 15, 2015*)
4. A policy should established prohibiting any data on the Vendor Master File that is connected to a staff member with update ability on the file. (*December 15, 2015*)

Management's Actions: Management has action plans to remedy the situations described above, with implementation dates as noted above.

II. Lab Safety and Security-15/16-001

Objectives included evaluation of lab safety training, periodic lab inspections, and physical security of the labs, and compliance with federal regulations. Audit fieldwork began on April 15, 2015, and ended on June 5, 2015. The audit report was issued on July 27, 2015.

Results:
The audit identified 5 findings as follow (*expected implementation dates are in parenthesis*):

1. Chemistry Storeroom policies and procedures should be finalized and disseminated to appropriate persons. (*September 1, 2015*)
2. EH&S policies should ensure all lab policies and procedures are available and easily accessible to users. (*August 31, 2015*)
3. Procedures should be developed to ensure that all lab faculty and staff attend appropriate training prior to beginning lab work. (*EH&S/CSEH will meet by August 31, 2015; full implementation by January 15, 2015*)
4. Lab managers should ensure that lab safety materials and equipment are appropriately located in the labs. Codes on lab door cypher locks should be updated periodically. (*Emergency equipment by July 31, 2015; lock code changes by September 1, 2015*)
5. Lab inspections should be performed by EH&S on a periodic basis. (*January 15, 2016*)

Management's Actions: Management has action plans to remedy each situation, as identified by the implementation dates noted above**.**

Recommendation: Acceptance of the Internal Auditing Reports

Implementation: Management will implement corrective actions. Internal Auditing will follow-up to determine if adequate corrective actions occurred.

Fiscal Implications: Fiscal oversight by the UWF Board of Trustees

---

Supporting documents:
UWF-14/15-006 Internal Auditing Report Vendor Master File
UWF-15/16-001 Internal Auditing Report Lab Safety and Security

Prepared by: Cindy Talbert, Interim Internal Audit Director, 474-2638, ctalbert@uwf.edu

Presenter: Cindy Talbert, Interim Internal Audit Director

EXECUTIVE SUMMARY

We audited the Vendor Master File for the period of January 1, 2014 through February 28, 2015. This audit was included as part of our 2014/15 audit work plan, determined by our annual risk assessment. Our objectives were to:

- Determine if adequate preventive internal controls are in place over vendor validation, setup, modification, and maintenance processes to protect the University from the creation and/or activation of unauthorized, duplicate, or unapproved vendors.
- Determine whether the University is in compliance with relevant statutes and regulations, and related departmental policies and procedures.
- Determine whether payments are made only to authorized and approved vendors.
- Verify that transaction activity within the vendor master accounts, including one-time vendors, is reviewed periodically and the accounts are updated appropriately.
- Determine if management is performing adequate due diligence when assessing new vendors.

Audit fieldwork began on January 13, 2015 and ended on May 15, 2015. Our audit was conducted in accordance with the Institute of Internal Auditors International Standards for the Professional Practice of Internal Auditing and generally accepted auditing standards.

BACKGROUND

The University of West Florida's (UWF) purchasing activities take place utilizing an electronic file of information about vendors. This information includes business names, addresses, employer identification numbers, contact information, and other vital bits of data. As various types of purchases are processed, such as requisitions, purchase orders, one-time payments, and credit card transactions, the UWF information system accesses these bits of information in order to make payments and to maintain a history of financial activities. The file in which all of this information is collected is referred to as the Vendor Master File.

UWF Procurement and Contracts has established two methods of vendor creation on the Vendor Master File. Vendor records can be established within the department, or vendors can initiate a process to create their own records using a web-based "Vendor Registration" connection. These externally-initiated vendor records are reviewed by Procurement and Contracts for accuracy and completeness before they are formally accepted as part of the Vendor Master File.

The Vendor Master File was previously maintained by the CICS information management system. In July 2004, this task was migrated to the Ellucian Banner Finance Information System.

Responsibility for oversight of the Vendor Master File has been assigned to the Procurement and Contracts department, where the Procurement Systems Specialist serves as the functional lead. Procurement and Contracts has developed a series of standard operating procedures, which lay out the specific guidelines on how vendors are to be registered, maintained, and accessed.

The Vendor Master File consists of 23,126 individual entries, which constitute 15,576 specific vendors; many vendors have multiple entries, usually associated with a change in address or business name. Of these vendor entries, 12,893 are active vendors and 2,683 are inactive vendors. Active vendors are coded such that financial transactions are eligible to be processed against them.

KEY OBSERVATIONS

The entirety of the Vendor Master File *(as of February 19, 2015),* along with relevant UWF policies and procedures, was reviewed and subsequently compared

against accepted best practices for vendor master file management. The audit revealed the following:

1. UWF has no policies designed in regards to de-activating vendors that are no longer in use, or have not been used in a significant duration of time. We noted that 54.1% (6,980) of active vendors have not had a payment processed since 2013; and 13.6% (1,758) of active vendors have never had a payment processed. Although purging and archiving one-time vendors and inactive vendors is a widely agreed-upon best practice for minimizing risks within the purchasing system, Information Technology Services (ITS) and Procurement and Contracts have elected to deactivate vendors (which prevents any activity) rather than archiving or purging due to the risks of losing historical data. In the alternative, deactivating these rarely used vendors would provide at least some level of additional control over their use in financial transactions.

2. Audit testing identified 77 potential duplicate vendors (or 1.1% of all active vendors). This conclusion is based upon textual similarities in combinations of data fields such as vendor name, address and federal employer Tax Identification Number (TIN). The existence of duplicate vendors in the file increases the risk of erroneous payments.

3. Our review of controls over the automated vendor registration system indicated that only a cursory review of new vendors is performed. Additional steps that might be taken to ensure the validity and propriety of using a vendor include utilizing the IRS Taxpayer Identification Number (TIN) On-Line Matching program. Another important step includes referring to the U.S. System for Awards Management Excluded Parties List (SAM EPLS). Our audit testing identified 2 active vendors that currently reside on this list that reports entities that have been federally suspended or debarred. Conducting business with the latter could result in serious penalties or loss of Federal funding.

4. Two Procurement and Contracts employees with modification access to the Vendor Master File, and with invoice approval privileges, are listed in the file as active vendors, in association with their roles as officers in local professional organizations. As such, no impropriety seems evident; however, this improper separation of duties creates the opportunity for unauthorized payments to be transacted.

Notable Strengths

We found two notable strengths within Procurement and Contracts during the course of the audit fieldwork. The Standard Operating Procedures developed for the management of the Vendor Master File were very thorough and provide an excellent resource in case of employee turnover. In addition, the Procurement and Contracts website was well-designed and maintained. It is filled with relevant guides and support documentation that proved to be a great source of information throughout the audit.

Suggested Management Actions

1. Procurement and Contracts, in cooperation with ITS, should develop a Standard Operating Procedure for annually deactivating any vendor that has not been used in the previous five years.

2. Procurement and Contracts should review the list of possible duplicate vendor accounts and either deactivate or combine accounts where appropriate. Additionally, we recommend that Procurement and Contracts establish an annual procedure, based on the testing processes such as those used in this audit, to annually identify and address any duplicate vendors that may have circumvented the system controls.

3. Procurement and Contracts should expand their background review of new vendors to include the application of the IRS's Taxpayer Identification Number (TIN) On-Line Matching program to ensure that "high-risk" vendors are validated, prior to use. Furthermore, in cooperation with ITS, they should develop a Standard Operating Procedure which requires that each month all active vendors are cross-referenced with the SAM EPLS database to ensure that no vendor is federally suspended or debarred.

4. Procurement and Contracts should remove all contact information belonging to Procurement and Contracts employees from the Vendor Master File. Furthermore, they should develop a policy stating that no employee with modification access to the Vendor Master File and the authority to influence or approve invoices can be allowed to register as a University vendor.

We appreciate the cooperation, professionalism, and responsiveness of the Procurement and Contracts and Information Technology Services staff who were involved in the audit.

Respectfully submitted,

Cynthia Talbert

Cynthia Talbert, CPA
Interim Internal Audit Director

Audit performed by: Matthew Packard

REPORT PROVIDED TO THE FOLLOWING:

Dr. Judy Bense, President
Lewis Bear, Chair BOT
Susan O'Connor, Chair Audit Committee
Bob Jones, Audit Committee
Dr. Pam Dana, Audit Committee
Dr. Martha Saunders, Provost and Executive Vice President
Dr. George Ellenberg, Vice Provost
Betsy Bowers, Interim Vice President
Angie Jones, Director, Procurement and Contracts
Melanie Haveard, Executive Director, ITS
Colleen Asmus, Controller
Pat Lott, General Counsel
Jim Stultz, Manager, FL Auditor General
Ken Danley, Supervisor, FL Auditor General
Joe Maleszewski, BOG Chief Inspector General
Lori Clark, BOG Compliance and Audit Specialist
Rebecca Luntsford, BOT Liaison

OBSERVATIONS WITH MANAGEMENT'S RESPONSES

Vendor Master File

UWF 14-15_006

OBSERVATION #1 WITH MANAGEMENT RESPONSE

What We Found	The University has no policies designed to deactivate inactive vendors or vendors that have not been accessed in a significant duration of time.
Why the Issue is Important	Effective management of the Vendor Master File will help guard the University against duplicate payments, IRS tax reporting errors and fines, and reduces the risk of becoming a victim of fraud.
What is Causing the Issue	Continuous vendor registration and a lack of a formal deactivation process has created a situation were approximately 51% of the vendors in the Vendor Master File have not received a payment since 2013 and approximately 14% of the vendors have not been used at all. ITS attempted a cleansing of inactive vendors in the past, but this led to complications and subsequent data loss. The data was eventually recovered, but the experience has left ITS hesitant to try this again.
What is Expected or Required	■ Vendors that have not been used in the previous five years should be de-activated.
What We Suggest	Procurement and Contracts, in cooperation with ITS, should develop a Standard Operating Procedure that establishes an annual process of deactivating vendors that have not been used in the previous five years.
Responsible Auditees	Angie Jones, Director, Procurement and Contracts Melanie Haveard, Executive Director, ITS
What Action Management Commits to Do	ITS and Procurement will work together to define the process for terminating inactive vendors in Banner. Procurement will provide ITS with the criteria for selecting vendor records to inactivate. Vendors will be inactivated by entering a termination date on their record in Banner. The proposal is to write a Banner process (in JOBSUB) that will allow Procurement to run the process in audit mode to find and review the list before actually terminating, and then in update mode to actually terminate inactive vendors in Banner. An SOP will be written to document the process.
Implementation Date	December 15, 2015

OBSERVATION #2 WITH MANAGEMENT RESPONSE

What We Found	Controls to prevent the creation of duplicate vendors could be improved upon.
Why the Issue is Important	Duplicate vendors are the leading cause of duplicate payments and can lead to inaccurate IRS tax reporting and missed vendor discounts. Attempting to recover duplicate payments can be costly and could be potentially damaging to the University's reputation.
What is Causing the Issue	Vendors frequently change their business names, addresses, merge with other companies or otherwise alter their vendor information. Without close scrutiny over manual data entry, automated system reviews and a manual periodic review process, preventing the creation of duplicate vendors can be extremely difficult.
What is Expected or Required	■ The Vendor Master File should be reviewed annually in order to identify any possible duplicate vendors that may have circumvented the established controls.
What We Suggest	Procurement and Contracts should annually perform a specialized review of the Vendor Master File to determine if any duplicate vendors exist. They should subsequently combine and/or deactivate vendors as appropriate.
Responsible Auditee	Angie Jones, Director, Procurement and Contracts
What Action Management Commits to Do	ITS and Procurement will work together to define the process for identifying duplicate vendors in Banner. The proposal is to either have ITS provide the download or give Procurement the ability to download an Excel document of vendor data that can be checked for duplicates. The current list of 77 duplicate vendors provided by IAMC for this audit has been researched and 57 duplicate records have been terminated, most of which were old entries when controls were not as stringent. An SOP will be written to annually identify and address any registration of duplicate vendors.
Implementation Date	December 15, 2015

OBSERVATION #3 WITH MANAGEMENT RESPONSE

What We Found	There are no validation procedures over the registration of new vendors.
Why the Issue is Important	A lack of a formal vendor approval process, one which should include the verification of vendors using the IRS's Taxpayer Identification Number (TIN) On-Line Matching program, leaves the University vulnerable to vendors that have poor performance/financial/reputational backgrounds. Additionally, by not verifying vendors against the System for Awards Management Excluded Parties System (SAM EPLS) the University risks penalties and the loss of Federal funding.
What is Causing the Issue	There is no policy or procedure established requiring the integrity of external vendors to be validated prior to use.
What is Expected or Required	■ All new vendors should be submitted to a formalized background check prior to being accepted into the Vendor Master file.
What We Suggest	Procurement and Contracts should expand their background review process to include the use of the IRS's Taxpayer Identification Number (TIN) On-Line Matching program on vendors deemed to be of high-risk to the University. Furthermore, in cooperation with ITS, they should develop a Standard Operating Procedure that establishes that, each month, the Vendor Master File is cross-referenced with the SAM EPLS to ensure UWF does not conduct business with a federally suspended or debarred entity.
Responsible Auditees	Angie Jones, Director, Procurement and Contracts Melanie Haveard, Executive Director, ITS
What Action Management Commits to Do	ITS and Procurement will work together to define the process for comparing vendors in Banner to the list of vendors found on the Excluded Parties List using TIN as the element to match vendors in the two systems. The proposal is to have Procurement staff download an Excel document of vendor data (preferably in a consistent format), which must include the TIN, to a specific folder and a Tableau report will be used to compare the vendors in the Excel file to vendors in Banner. An SOP will be written to document the process.
Implementation Date	December 15, 2015

OBSERVATION #4 WITH MANAGEMENT RESPONSE

What We Found	Certain employees with modification access to the Vendor Master File and the ability to approve invoices have personal addresses in the Vendor Master File.
Why the Issue is Important	This constitutes an improper separation of duties and creates the opportunity for unauthorized payments to be transacted.
What is Causing the Issue	There is no policy explicitly stating that employees with modification access to the Vendor Master File and the authority to approve or influence invoices cannot be allowed to register as a vendor.
What is Expected or Required	Establish policies to ensure that any employee with modification access and influence over invoicing is not allowed to register as a vendor in the Vendor Master File.
What We Suggest	Procurement and Contracts should develop a policy clearly stating that no employee with modification access to the Vendor Master File and the authority to influence or approve invoices can be allowed to register as a University vendor. Also, they should remove all contact information belonging to Procurement and Contracts employees.
Responsible Auditee	Angie Jones, Director, Procurement and Contracts,
What Action Management Commits to Do	Procurement has inactivated the current address information and added the new contact information to include the Association and University address for the two Procurement & Contracts employees from the Vendor Master File. Both of these entries are due to the Treasurer positions they hold in their respective associations. An SOP will be created to address the prohibition of anyone who has vendor modification access to be allowed to register as an active vendor.
Implementation Date	December 15, 2015

Internal Auditing & Management Consulting
Audit: Lab Safety and Security
Report #: UWF15-16_001
Date: July 27, 2015

EXECUTIVE SUMMARY

We audited lab safety and security for the period April 1, 2014 through March 31, 2015. This audit was included as part of our 2014/15 audit work plan, determined by our annual risk assessment. Our objectives were to:

- Verify the existence of an adequate safety training program.
- Assess the existence and adequacy of operational procedures and equipment to control any hazardous substances.
- Confirm that adequate controls exist over the physical security of the laboratories and assets.
- Verify adherence with OSHA requirements and the use of Material Safety Data Sheets (MSDS).

Audit fieldwork began on April 15, 2015 and ended on June 5, 2015. Our audit was conducted in accordance with the Institute of Internal Auditors International Standards for the Professional Practice of Internal Auditing and generally accepted auditing standards.

BACKGROUND

The University of West Florida has 73 laboratories (labs) on the main campus, including 47 non-classroom and open labs (includes 6 labs in the Center for Environmental Diagnostics and Bioremediation (CEDB)) and 29 classroom labs.

The Environmental Health and Safety Department (EH&S) has overarching responsibility for lab safety policies and training for lab personnel. EH&S staff are trained in chemical hygiene and hazardous waste management. Persons working in the labs must attend EH&S lab safety and hazardous waste training prior to beginning work and on an annual basis thereafter.

The following agencies perform inspections of UWF and EH&S related to lab safety and security:

- Fire marshal: fire code inspections
- Department of Environmental Health: hazardous waste
- Environmental Protection Agency: hazardous waste
- Florida Department of Health: radioactive waste
- Escambia County Department of Health: biohazardous waste
- Department of Homeland Security
- Florida Division of Risk Management: occupational safety

The Chemistry department maintains a central storage area for chemicals used in the Chemistry, Biology, and CEDB teaching labs. The lab manager receives the chemicals for all three departments, and secures, stores, and distributes the supplies as needed for classroom instruction.

Hazardous wastes are collected, stored temporarily on campus and disposed through the use of a private contractor.

KEY OBSERVATIONS

Of the 73 labs on campus, 12 (16%) were reviewed for safety, security, and emergency equipment. Training records were examined for 16 of 156 (10%) lab faculty and teaching assistants. The audit revealed the following opportunities for improvement:

1. Chemistry Storeroom policies and procedures had been drafted for a lengthy period of time but not been approved and disseminated to personnel.
2. EH&S department policies and procedures for labs existed, but were not made available on-line for lab personnel, which would provide ready access and improve compliance.
3. Of the 16 records reviewed, 3 individuals (16%) had not completed the required EH&S facilitated lab safety courses.
4. Twelve labs were reviewed and two (12%) had missing safety equipment. Codes for cypher security locks were not changed regularly as users changed over time.
5. No documentation was found in EH&S files that required annual lab inspections by EH&S had been conducted for the last few years.

NOTABLE STRENGTHS

EH&S staff members are well-qualified to administer the lab safety program. The Coordinator is credentialed by the Board of Certified Safety Professionals as a Certified Environmental, Safety and Health Trainer. The Environmental Coordinator attends annual instructional training for hazardous waste management, radiation safety, and laser safety.

SUGGESTED MANAGEMENT ACTIONS

Below is a summary of suggested actions, which would serve to strengthen the overall control environment:

- Departmental procedures related to the Chemistry Storeroom should be formalized and disseminated among users using appropriate media.
- The EH&S department should ensure all policies and procedures are available and easily accessible to users.
- Procedures should be developed and implemented to ensure all lab faculty and staff attend the appropriate initial and annual refresher training prior to beginning lab work.

- Lab managers should ensure required lab safety materials and equipment are appropriately located in labs. Codes on cypher locks should be updated immediately upon the change in personnel and on a periodic basis.

- Lab inspections should be performed by EH&S on a periodic basis.

We appreciate the cooperation, professionalism, and responsiveness of the University of West Florida staff who were involved in the audit.

Respectfully submitted,

Cynthia Talbert

Cynthia Talbert, CPA
Interim Internal Audit Director

Audit performed by: Dan Bevil

REPORT PROVIDED TO THE FOLLOWING:

Dr. Judith A. Bense, President
Lewis Bear, Chair BOT
Susan O'Connor, Chairperson, Audit Committee
Bob Jones, Audit Committee
Dr. Pam Dana, Audit Committee
Dr. Martha Saunders, Provost and Executive Vice President
Dr. George Ellenberg, Vice Provost
Betsy Bowers, Interim Vice President, Business, Finance, and Facilities
Dr. Michael Huggins, Dean, College of Science, Engineering, and Health
Dr. Matthew Schwartz, Chairperson, Environmental Studies and Chemistry
Dr. Christopher Pomory, Interim Chairperson, Biology
John Warren, UWF Police Chief
Peter Robinson, Director, Environmental Health and Safety
Pat Lott, General Counsel
Jim Stultz, Manager, FL Auditor General
Ken Danley, Supervisor, FL Auditor General
Joe Maleszewski, BOG Chief Inspector General
Lori Clark, BOG Compliance and Audit Specialist
Rebecca Luntsford, BOT Liaison

OBSERVATIONS
WITH
MANAGEMENT'S
RESPONSES

Lab Safety and Security
UWF15-16_001

OBSERVATION #1 WITH MANAGEMENT RESPONSE

What We Found	**Policies and Procedures** The Chemistry Storeroom policies have not been fully approved by departmental leadership.
Why the Issue is Important	Written policies and procedures create greater efficiency and productivity, provide clear understanding of job duties, and help ensure a smoother transition during staff turnover. Failure to have detailed procedures increases the risk of noncompliance.
What is Causing the Issue	Storeroom policies have not been fully vetted through applicable departmental leadership.
What is Expected or Required	Departmental policies and procedures should describe in detail the day-to-day activities of the operation, be written, signed by the organization leader, and made fully available to staff.
What We Suggest	The Chemistry department should revise the Storeroom policies as necessary, obtain the requisite approvals, and appropriately post the policies in a manner accessible for all concerned users.
Responsible Auditees	Dr. Matt Schwartz, Chairperson, Chemistry Dr. Alan Schrock, Associate Chairperson, Chemistry
What Action Management Commits To Do	The departmental storeroom policies are under review. When finalized, the policies will be disseminated among users.
Implementation Date	September 1, 2015

OBSERVATION #2 WITH MANAGEMENT RESPONSE

What We Found	**Policies and Procedures** The Environmental Health and Safety department's policies and procedures are not published on the UWF intranet.
Why the Issue is Important	The EH&S department is the office responsible for creation and dissemination of policies regarding lab safety at UWF. To maintain a safe work environment, it is important that faculty and staff have easy access to policies. Without the availability of policies, misunderstandings about proper safety procedures can arise and create unsafe conditions.
What is Causing the Issue	The University recently migrated its departmental websites to a new platform. During this system update, the EH&S website was not developed by departmental personnel and much of the important content was no longer made available.
What is Expected or Required	UWF departments should fully utilize the University intranet to circulate information across campus. The intranet is the best way to make information available for faculty and staff that are geographically dispersed.
What We Suggest	The EH&S department should post all policies and procedures on its website in a user friendly format.
Responsible Auditees	Peter Robinson, Director, Environmental Health and Safety
What Action Management Commits To Do	Environmental Health and Safety provided the pertinent information to the web administrator. Laboratory specific documents will be housed in a new tab on the website labeled "Laboratories."
Implementation Date	August 31, 2015

OBSERVATION #3 WITH MANAGEMENT RESPONSE

What We Found	**Training** The EH&S lab safety training courses were not completed for one faculty member and two Teaching Assistants, 16% of those reviewed.
Why the Issue is Important	Regulatory agencies and UWF policies require anyone working around hazardous materials to have proper safety training.
What is Causing the Issue	There is a lack of record keeping and follow up to ensure staff members and assistants have attended the required trainings prior to beginning work in the laboratories, especially for returning assistants and those attending annual refresher training.
What is Expected or Required	Training should be provided to employees to ensure they are apprised of the chemical hazards present in the lab environment.
What We Suggest	EH&S and the laboratory leadership should collaborate to develop and implement procedures to ensure all lab faculty and staff attend the appropriate training and annual refresher courses prior to beginning lab work.
Responsible Auditees	Dr. Michael Huggins, Dean, College of Science, Engineering, and Health Peter Robinson, Director, Environmental Health and Safety
What Action Management Commits To Do	The Environmental Health and Safety Department will meet with the College of Science, Engineering, and Health to identify the processes needed to ensure all faculty and staff working in labs are fully trained.
Implementation Date	Meeting: August 31, 2015 Full implementation of procedures: January 15, 2015

OBSERVATION #4 WITH MANAGEMENT RESPONSE

What We Found	**Lab Safety** Lab inspections revealed: missing emergency contact sheet; MSDSs; first aid kit; and the absence of regular code updates to lab cypher locks.
Why the Issue is Important	Regulatory agencies and UWF policies require safety equipment, contact information, and MSDSs easily accessible to those in the lab. Best practices for security recommend changes to the pass codes upon a personnel change.
What is Causing the Issue	The absence of periodic lab inspections makes it possible for safety issues to go unnoticed.
What is Expected or Required	In accordance with UWF EH&S Chemical Hygiene Program Manual and OSHA standards, MSDSs and first aid kits should be easily accessible in every lab and emergency contact information should be posted on the outside door of every lab and chemical storage area. Cypher lock codes combinations should be updated immediately upon the change of staff members and historical records should be maintained of all changes.
What We Suggest	The appropriate lab managers should ensure MSDSs , emergency contact information, and first aid kits are supplied to all labs. Code combinations for cypher locks should be changed immediately upon the termination of lab staff and on a periodic basis. For audit and security purposes, historical records should be maintained of those updates.
Responsible Auditees	Dr. Christopher Pomory, Interim Chairperson, Biology Dr. Matt Schwartz, Chairperson, Chemistry Dr. Alan Schrock, Associate Chairperson, Chemistry
What Action Management Commits To Do	A process is underway to review all labs and ensure the availability of proper emergency equipment and materials. The Chemistry Department has issued a departmental policy dated July 24, 2015 requiring that all Chemistry keyless lock codes on lab doors be changed at the end of every semester and immediately upon departure of research staff.
Implementation Date	Emergency equipment: July 31, 2015 Keyless lock codes: September 1, 2015

OBSERVATION #5 WITH MANAGEMENT RESPONSE

What We Found	**Lab Inspections** Periodic lab inspections were not performed during the audit period.
Why the Issue is Important	UWF Chemical Hygiene Program Manual states that the Director of EH&S will conduct periodic inspections to ensure compliance with the Chemical Hygiene Program.
What is Causing the Issue	Resource limitations in the EH&S department encumbered the lab inspection process.
What is Expected or Required	Compliance with the Chemical Hygiene Program Manual.
What We Suggest	EH&S should inspect all UWF labs, develop a program of continued inspections on a frequency of no less than one each calendar year, and maintain historical documentation of inspections.
Responsible Auditee	Peter Robinson, Director, Environmental Health and Safety
What Action Management Commits To Do	Environmental Health and Safety have begun formal inspections of labs on the UWF main campus. Currently we plan to inspect 12 labs per month.
Implementation Date	January 15, 2016

Agenda Item

UWF Board of Trustees Meeting
Audit & Operations Committee
August 5, 2015

Issue: BOT-13.01-09/15 Identity Theft Prevention Policy

Proposed action: Approval

Background information:

The University of West Florida ("University") established and maintains an Identity Theft Prevention Program ("Program") pursuant to the Federal Trade Commission's ("FTC") Red Flags Rule, which implements Section 114 of the Fair and Accurate Credit Transactions Act of 2003. The Program was approved by the Board of Trustees on March 6, 2009. This policy reflects the Program requirements.

Recommendation:

That the Board of Trustees approve the attached University Policy, BOT-13.01-09/15 Identity Theft Prevention.

Implementation Plan:

The policy has been posted for review and comment in the University's PCRA system and included in the University's published policies pending approval by the Board. Because the policy reflects an existing Board approved Program, implementation has been accomplished.

Fiscal Implications:

Supporting documents: BOT-13.01-09/15 Identity Theft Prevention Policy

Prepared by: **Patricia Lott, General Counsel, 850.474.3419,** plott@uwf.edu

Facilitator/Presenter: **Patricia Lott, General Counsel**

University Policy BOT-13.01-09/15

Policy Title: Identity Theft Prevention Policy

Originator: Dr. Judith A. Bense, President

Responsible Office: University Risk and Compliance Council

Reason for Policy/Purpose:

This policy sets forth the University of West Florida Identity Theft Prevention Program.

The University of West Florida ("University") established and maintains an Identity Theft Prevention Program ("Program") pursuant to the Federal Trade Commission's ("FTC") Red Flags Rule, which implements Section 114 of the Fair and Accurate Credit Transactions Act of 2003. The Program was developed for the University with the oversight of the University of West Florida Board of Trustees and was approved by the Board of Trustees on March 6, 2009.

Who Does this Govern and Who Needs to Know this Policy?

All University personnel involved in the processing of personally identifying information as applied to the administration of Covered Accounts.

Definition of Terms:

Identifying Information: Any name or number that may be used alone or in conjunction with any other information to identify a specific person, including: name, address, telephone number, social security number, date of birth, driver's license or identification number, alien registration number, passport number, employer or taxpayer identification number.

Identity Theft: A fraud committed or attempted using the identifying information of another person without authority.

Red Flag: A pattern, practice or specific activity that indicates the potential for Identity Theft.

Covered Account: An account used mostly for personal, family, or household purposes, and that involves multiple payments or transactions. A Covered Account is also an account for which there is a foreseeable risk of Identity Theft.

Program Administrator: the individual designated to have primary responsibility for oversight of the Program.

Processes:

I. Fulfilling Requirements of the Red Flags Rule.

Under the Red Flags Rule, the University is required to establish an Identity Theft Prevention Program tailored to its size, complexity, and the nature of its operation. This Program must contain reasonable policies and procedures to:

A. Identify relevant Red Flags for new and existing Covered Accounts and incorporate those Red Flags into the Program.

B. Detect Red Flags that have been incorporated into the Program.

C. Respond appropriately to any Red Flags that are detected to prevent and mitigate Identity Theft.

D. Ensure the Program is updated periodically to reflect changes in risks to individuals or to the safety and soundness of the individuals from Identity Theft.

II. Identification of Red Flags.

To identify relevant Red Flags, the University considers the types of accounts that it offers and maintains, methods it provides to open its accounts, methods it provides to access its accounts, and its previous experiences with Identity Theft. The University identifies the following Red Flags in each of the listed categories:

A. Notifications and Warnings from Credit Reporting Agencies.

1. Report of fraud accompanying a credit report.

2. Notice or report from a credit agency of a credit freeze on an applicant.

3. Notice or report from a credit agency of an active duty alert for an applicant.

4. Receipt of a notice of address discrepancy in response to a credit report request.

5. Indication from a credit report of activity that is inconsistent with an applicant's usual pattern or activity.

B. Suspicious Documents.

1. Identification document or card that appears to be forged, altered, or inauthentic.

2. Identification document or card on which a person's photograph or physical description is not consistent with the person presenting the document.

3. Other document with information that is not consistent with existing identifying information.

4. Application for service that appears to have been altered or forged.

C. Suspicious Personal Identifying Information.

1. Identifying information presented that is inconsistent with other information provided (example: inconsistent birth dates).

2. Identifying information presented that is inconsistent with other sources of information (for instance, an address not matching an address on a loan application).

3. Identifying information presented that is the same as information shown on other applications that were found to be fraudulent.

4. Identifying information presented that is consistent with fraudulent activity (such as an invalid phone number or fictitious billing address).

5. Social security number presented that is the same as one given by another person.

6. An address or phone number presented that is the same as that of another person.

7. A person fails to provide complete personal identifying information on an application when reminded to do so.

8. A person's identifying information is not consistent with the information that is on file for that person.

D. Suspicious Covered Account Activity or Unusual Use of Account.

1. Change of address for an account followed by a request to change the person's name.

2. Payments stop on an otherwise consistently up-to-date account.

3. Account used in a way that is not consistent with prior use.

4. Mail sent to the individual is repeatedly returned as undeliverable.

5. Notice to the University that a person is not receiving mail sent by the University.

6. Notice to the University that an account has unauthorized activity.

7. Breach in the University's computer system security.

8. Unauthorized access to or use of student account information.

E. Alerts from Others.

Notice to the University from an individual, Identity Theft victim, law enforcement official, or other person that the University has opened or is maintaining a fraudulent account for a person engaged in Identity Theft.

III. Detecting Red Flags.

A. Student Enrollment.

To detect any of the Red Flags identified above associated with the enrollment of a student, University personnel will take the following steps to obtain and verify the identity of the person opening the account:

1. Require certain identifying information such as name, date of birth, academic records, home address, or other identification; and

2. Verify the student's identity at time of issuance of identification card (review of driver's license or other government-issued photo identification).

B. Existing Accounts.

To detect any of the Red Flags identified above for an existing Covered Account, University personnel will take the following steps to monitor transactions on an account:

1. Verify the identification of the individual if they request information (in person, via telephone, via facsimile, via email).

2. Verify the validity of requests to change billing addresses by mail or email and provide the individual a reasonable means of promptly reporting incorrect billing address changes.

3. Verify changes in banking information given for billing and payment purposes.

C. Consumer Credit Report Requests.

To detect any of the Red Flags identified above for an employment or volunteer position for which a credit or background report is sought, University personnel will take the following steps to assist in identifying address discrepancies:

1. Require written verification from any applicant that the address provided by the applicant is accurate at the time the request for the credit report is made to the consumer reporting agency.

2. In the event that notice of an address discrepancy is received, verify that the credit report pertains to the applicant for whom the requested report was made and report to the consumer reporting agency an address for the applicant that the University has reasonably confirmed is accurate.

IV. Preventing and Mitigating Identity Theft.

In the event that University personnel detect any identified Red Flags, such personnel shall take one or more of the following steps, depending on the degree of risk posed by the Red Flag:

A. Prevent and Mitigate.

1. Continue to monitor a Covered Account for evidence of Identity Theft.

2. Contact the individual (for which a credit or background report was run).

3. Change any passwords or other security devices that permit access to Covered Accounts.

4. Not open a new Covered Account.

5. Provide a new identification number.

6. Notify the Program Administrator for determination of the appropriate step(s) to take.

7. Notify law enforcement.

8. File or assist in filing a Suspicious Activities Report.

9. Determine that no response is warranted under the particular circumstances.

B. Protect Student Identifying Information.

In order to further prevent the likelihood of Identity Theft occurring with respect to Covered Accounts, the University will take the following steps with respect to its internal operating procedures to protect student identifying information:

1. Ensure that its website is secure or provide clear notice that the website is not secure.

2. Subject to state record retention requirements, ensure complete and secure destruction of paper documents and computer files containing account information when a decision has been made to no longer maintain such information.

3. Ensure that office computers with access to Covered Account information are password protected.

4. Avoid use of social security numbers whenever possible.

5. Ensure that computer virus protection is up to date.

6. Require and keep only the kinds of personally identifying information that are necessary for University purposes.

C. Program Administration.

1. Oversight.

Responsibility for developing, implementing and updating this Program lies with an Identity Theft Committee ("Committee") for the University. The University's Risk and Compliance Council presently serves as the Committee. The Committee is headed by a Program Administrator who may be the President of the University or his or her appointee. Two or more other individuals appointed by the President of the University or the Program Administrator comprise the remainder of the committee membership. The Program Administrator is responsible for ensuring appropriate training of University staff on the Program, for reviewing any staff reports regarding the detection of Red Flags and the steps for preventing and mitigating Identity Theft, determining which steps of prevention and mitigation should be taken in particular circumstances and considering periodic changes to the Program.

2. Staff Training and Reports.

University staff responsible for implementing the Program shall be trained in the detection of Red Flags and the responsive steps to be taken when a Red Flag is detected. University staff shall be trained, as necessary, to effectively implement the Program. University employees are expected to notify the Program Administrator and University Internal Auditing and Management Consulting once they become aware of an incident of Identity Theft or of the University's failure to comply with this Program. At least annually or as otherwise requested by the Program Administrator, University staff responsible for implementation and administration of the Program shall report to the Program Administrator on compliance with this Program. The report should address such issues as effectiveness of the policies and procedures in addressing the risk of Identity Theft in connection with the opening and maintenance of Covered Accounts, service provider arrangements, significant incidents involving Identity Theft, management responses, and recommendations for changes to the Program.

3. Service Provider Arrangements.

In the event the University engages a service provider in performing an activity in connection with one or more Covered Accounts, the University will take the following steps to ensure the service provider performs its activity in accordance with reasonable policies and procedures designed to detect, prevent, and mitigate the risk of Identity Theft.

a. Require, by contract, that service providers have such policies and procedures in place; and

b. Require, by contract, that service providers review the University's Program and report any Red Flags to the Program Administrator or the University employee with primary oversight of the service provider relationship.

4. Non-disclosure of Specific Practices.

For the effectiveness of this Identity Theft Prevention Program, knowledge about specific Red Flag identification, detection, mitigation, and prevention practices may need to be limited to the Committee members who developed this Program and to those employees who need to know them. Any

documents that may have been produced or are produced in order to develop or implement this Program that list or describe such specific practices and the information those documents contain are considered confidential and should not be shared with other University employees or the public, unless required by applicable law. The Program Administrator shall identify those documents and practices that should be maintained in a confidential manner.

5. Program Updates.

The Committee will periodically review and update this Program to reflect changes in risks to individuals and the soundness of the University from Identity Theft. In doing so, the Committee will consider the University's experiences with Identity Theft situations, changes in Identity Theft methods, changes in Identity Theft detection and prevention methods, and changes in the University's business arrangements with other entities. After considering these factors, the Program Administrator will determine whether changes to the Program, including the listing of Red Flags, are warranted. If warranted, the Committee will update the Program.

Change Justification:

This is a new policy. This policy restates the University's Identity Theft Prevention Program adopted by the University of West Florida Board of Trustees on March 6, 2009.

Authority and Related Documents:

Federal Trade Commission's Red Flags Rule, 16 C.F.R. 681 and Section 114 of the Fair and Accurate Credit Transactions Act, 15 U.S.C. 1681m(e).

APPROVED: _____ **Date:** _____

Dr. Judith A. Bense, President

History:

Scheduled for Ratification by the University of West Florida Board of Trustees on September 30, 2015.

Action Item

BOT AGENDA RECOMMENDATION SUBMISSION

UWF Board of Trustees Meeting
Audit and Operations Committee
August 5, 2015

Issue/Agenda Recommendation: Approval of Revised UWF Human Resources Policy HR-20.02-07/15 *Recruitment, Selection, and Appointment*

Proposed Action: Approve

Background Information:

The Human Resources Department, in conjunction with the General Counsel's Office, is continuously reviewing and revising UWF Human Resources policies.

Human Resources policy HR-20.02-07/15 *Recruitment, Selection, and Appointment* was originally adopted by the UWF Board of Trustees in July, 2004. This policy was revised and sent to campus for public review and comment from June 10, 2015, to July 10, 2015.

Feedback was received and changes were made based on the feedback received.

Implementation Plan: When approved by the Board of Trustees, new or revised policies will be placed on the Human Resources web site HR policy section. Announcements will be placed in the Human Resources electronic newsletter, *HR Bulletin*.

Fiscal Implications: None

Supporting documents: None

Prepared by: Jamie Sprague, Associate Director, Human Resources Department, 850-474-2156, jsprague@uwf.edu

Facilitator/Presenter: Jamie Sprague, Associate Director, Human Resources Department, 850-474-2156, jsprague@uwf.edu

University Policy HR-20.02-07/15 Summarized Changes

The following changes have been proposed for this policy:

- Gender identity was added to the policy to align with the University's non-discrimination policy.

- Appointment types for Faculty and University Work Force were updated to align with current practices and clarified. Clarified and expanded provisions for OPS positions.

- Changed advertising minimum from 5 working days to 10 working days. A referenced to E-verify was added to the advertising section.

- All Faculty and University Work Force line positions must be advertised in at least one external publication targeted to recruit gender and racial/ethnic minority candidates.

- The provisions related to search committees were substantially changed.
  - Hiring officials are now required to utilize a search committee in the hiring of any ranked Faculty position and for any University Work Force position at the director level or higher. The hiring official may, but is not required, to utilize a search committee for an adjunct, instructor, or lecturer position. The same is true for a position below a director. The existing policy required search committees for all positions.

  - Whenever a search committee is utilized in a search, the recruitment will follow the Florida Sunshine meeting requirements. The existing policy only required search committees to follow Florida Sunshine meeting requirements where the law required that the Sunshine law be followed.

  - Re-defined the composition of a search committee.

- Clarified and expanded the exemptions from and waivers of recruitment provisions.

- Explained the applicant pool certification process and clarified current practices.

- Updated application process provisions to reflect current processes and changes in the law.

- Clarified that offer letters for University Work Force positions must be approved by Human Resources before being sent to the finalist and that offer letters for Faculty positions must be approved by the Provost's office before being sent to the finalist.

- Selection and appointment provisions have been added to provide guidance about the timing of the offer and conditions such as background screens and reference checks.

- Information about background screens/checks has been added to reflect changes in the law.

Informational Item

UWF Board of Trustees Meeting
Audit & Operations Committee
August 5, 2015

Issue: Internal Auditing Update on Activities
Proposed action: Informational

To provide the Committee with an overview of activities within Internal Auditing and Management Consulting.

1. Status of audits in process
2. Status of advisory/consulting activities
3. External Audits performed by outside parties (none)
4. Compliance operation
5. Miscellaneous items

Recommendation: None

Implementation: None

Fiscal Implications: Fiscal oversight by the UWF Board of Trustees

---

Prepared by: Cindy Talbert, Interim Internal Audit Director, 474-2638, ctalbert@uwf.edu

Presenter: Cindy Talbert, Interim Internal Audit Director

UWF Flood Disaster
Financial Summary as of July 27, 2015

Estimate of damages:			
University			$ 1,095,674
Housing			31,822
Direct Support Organizations (Arcadia Mills, Historic Trust)			15,761
Total of estimated damages			$ 1,143,257
Less reimbursement received:			
Florida Division of Risk Management	$	256,975	
Department of Emergency Management		27,807	
Emergency Watershed Protection Grant		461,141	
FEMA		-	
Total reimbursement received			(745,923)
Unreimbursed damages			$ 397,334
Less amount projected to be reimbursed (net*)			(222,894)
Estimated loss to UWF as of July 27, 2015			$ 174,440

*Duplicate payment from Dept. of Risk Management and FEMA will be reimbursed.