Geological Sciences Department

Change in Management Audit

Audit Report # 16-08

June 20, 2016

The University of Texas at El Paso
Institutional Audit Office

”Committed to Service, Independence and Quality”

THE UNIVERSITY of TEXAS SYSTEM
FOURTEEN INSTITUTIONS. UNLIMITED POSSIBILITIES.

UTEP Institutional Audit Office
500 West University Ave.
El Paso, Texas 79968
915-747-5191
WWW.UTEP.EDU
WWW.UTSYSTEM.EDU

June 20, 2016

Dr. Diana Natalicio
President, University of Texas at El Paso
Administration Building, Suite 500
El Paso, Texas 79968

Dear Dr. Natalicio:

The Office of Auditing and Consulting Services has completed a Change in Management audit of the Geological Sciences Department. During the audit, we identified opportunities for improvement and offered the corresponding recommendations in the audit report. The recommendations are intended to assist the department in strengthening controls and help ensure that the University's mission, goals and objectives are achieved.

We appreciate the cooperation and assistance provided by the Geological Sciences Department during our audit.

Sincerely,

Lori Wertz

Lori Wertz
Chief Audit Executive

Report Distribution:

University of Texas at El Paso:
Mr. Richard Adauto III, Executive Vice President
Dr. Howard Daudistel, Interim Provost, Vice Provost for Academic Affairs (VPAA)
Dr. James Kubicki, Chair, Geological Sciences Department
Dr. Robert Kirken, Dean, College of Science
Mr. Gerard Cochrane, Chief Information Security Officer
Ms. Sandra Vasquez, Assistant Vice President for Equal Opportunity (EO) and Compliance

University of Texas System (UT System):
System Audit Office

External:
Governor's Office of Budget, Planning and Policy
Legislative Budget Board
Internal Audit Coordinator, State Auditor's Office
Sunset Advisory Commission

Audit Committee Members:
Mr. David Lindau
Mr. Steele Jones
Mr. Fernando Ortega
Dr. Stephen Riter
Dr. Roberto Osegueda

Auditors Assigned to the Audit:
Mirna Naylor, Auditor
Narahay Buendia, Auditor
Victoria Morrison, IT Auditor

Table of Contents

EXECUTIVE SUMMARY

The Office of Auditing and Consulting Services (OACS) has completed a limited scope Change in Management Audit of the Geological Sciences Department. The audit scope was limited to selected fiscal and administrative activities for the period of September 1, 2014 through January 31, 2016. The objectives of this audit were to determine whether the Department is operating in a control-conscious environment, to verify that the audited areas are in compliance with University policies and procedures, and to identify opportunities for improvement.

During the audit we noted the following:

- The Geological Sciences Department does not have documented policies and procedures. Policies and procedures are the strategic link between the office vision and the effective performance of its day-to-day operations.

- The Department is not in compliance with The University of Texas at El Paso's Procurement Card Policy. One cardholder reconciled his own Pro-card transactions and did not submit the reconciliation to the supervisor for approval. Unallowable transactions were identified by the Purchasing Department and the employee was required to reimburse the money to The University.

- One employee's eligibility to work was not verified prior to employment. The employee started working at the Geological Sciences Department before the Human Resources Department was notified and before the required background check was completed.

- Monthly account reconciliations were not consistently prepared, reviewed and approved as required by University policies and procedures.

- The Department is not following University regulations regarding collection of donation funds.

- Three appointments, four supplemental payments and two changes in contract amounts were processed late due to delayed submission of information by the Geological Sciences Department to the Human Resources Office.

- Backup/restore controls are not being followed and/or need process improvements to safeguard against loss of data.

EXECUTIVE SUMMARY (CONT'D)

- There is no contingency plan to eliminate the risk of a single point of failure in case of the permanent absence of the System Administrator.

- Security safeguard software is not installed in accordance with Texas Security Controls Standards Catalog Version 1.3 (TAC 202.76 Security Control Standards Catalog); therefore, PCs are not fully protected from threats.

- There is lack of communication and security oversight with the Information Security Office (ISO), which could render the system vulnerable to internal and external threats.

- The Geology Department has not documented the identified mission critical resources and computing assets necessary to recover hardware, applications and data in case of a disaster.

- OACS found that of 18 servers running mission critical systems, three have operating systems which are at or near end of life. End of life/support means that the software vendor will no longer provide fixes, security updates, service packs, or online technical support.

BACKGROUND

The Department of Geological Sciences at The University of Texas at El Paso (UTEP) consists of tenured and tenure-track faculty with research areas focused under five main themes: earth surface processes and geochemistry, economic geology and energy resources, geo-informatics and technology, geophysics, and tectonics and sediment dynamics.

The department offers degree programs in both Geological Sciences and Environmental Sciences in conjunction with faculty from the Biological Science and Chemistry Departments.

Dr. James Kubicki joined the College of Science as Chair of the Department of Geological Sciences at UTEP, on August 1, 2015.

AUDIT OBJECTIVES

The objectives of this audit were to determine:

A. the level of internal control awareness,

B. whether administrative and financial operations are performed in accordance with University policies and procedures, and

C. whether the Department of Geological Sciences, Dean's Office, operates in compliance with the UTEP Information Security Policy.

SCOPE AND METHODOLOGY

The audit was conducted in accordance with the *International Standards for the Professional Practice of Internal Auditing* issued by the Institute of Internal Auditors.

Audit procedures included performing a risk analysis, reviewing departmental policies and procedures, interviewing personnel, identifying significant accounts, and assessing the account reconciliation process. Testing on a sample basis was performed in the areas of salaries and wages, expenditures, Procard, asset management, and IT security to verify the effectiveness of internal controls, and compliance with the University's administrative and financial policies and procedures. The scope of the audit is September 1, 2014 through January 31, 2016.

RANKING CRITERIA

All findings in this report are ranked based on an assessment of applicable qualitative, operational control and quantitative risk factors, as well as the probability of a negative outcome occurring if the risk is not adequately mitigated. The criteria for the rankings are as follows:

Priority – An issue identified by an internal audit that, if not addressed timely, could directly impact achievement of a strategic or important operational objective of a UT institution or the UT System as a whole.

High – A finding identified by internal audit that is considered to have a medium to high probability of adverse effects to the UT institution either as a whole or to a significant college/school/unit level.

Medium – A finding identified by internal audit that is considered to have a low to medium probability of adverse effects to the UT institution either as a whole or to a college/school/unit level.

Low – A finding identified by internal audit that is considered to have minimal probability of adverse effects to the UT institution either as a whole or to a college/school/unit level.

AUDIT RESULTS

A. Level of Internal Controls

According to the Committee of Sponsoring Organizations of the Treadway Commission, internal controls are designed by the board of directors and management to provide reasonable assurance regarding the achievement of objectives relating to operations, reporting and compliance.

A. Policies and Procedures

Policies and procedures are part of an organization's internal controls. They are used as a communication tool with a main purpose of guiding managers and supervisors in making decisions, training personnel and handling employment issues. They are the strategic link between the institution's vision, and its day-to-day operations, identify key activities and provide an easily understood plan of action required to carry out organizational operations. These policies must be consistent with the organization's guidelines and any pertinent regulatory or other requirements.

The Geological Sciences Department does not have documented goals, policies and procedures.

***Recommendation**:*
The Geological Sciences Department should document goals and objectives and develop a policies and procedures manual to reflect the administrative, financial and information technology operations of the Department, to provide guidance to employees, and to ensure alignment with University mission and goals.

Level: This finding is considered **Medium** risk due to the probability that daily operations could not be carried out on a timely basis, and the possibility of costly mistakes due to lack of clear guidance.

Management Response:
The policies and procedures are being revised to reflect the updates to PeopleSoft and any changes that may have been implemented by the University.

Responsible Party:
Kristen Gonzalez, Administrative Services Coordinator
Carlos Montana, System Administrator

***Implementation Date:** March 31, 2017*

B. Administrative and Fiscal Operations

B.1 Compliance with Procard Policies

According to the UTEP Procurement Card Program Policy;

> *"The cardholder is ultimately responsible for verifying that all transactions listed on the statements are valid…*
>
> *It is the reconciler's responsibility to monitor and reconcile all transactions in PeopleSoft and update transaction logs …*
>
> *Lastly, at the end of each cycle, the corresponding transaction log must be signed and dated by the supervisor within one months' time of the monthly PeopleSoft reconciliation being issued."*

The Department is not in compliance with UTEP's Procurement Card Policy. One cardholder reconciles his own procard transactions and does not submit the reconciliation to the supervisor for approval.

The statements for the months of August and October 2015 displayed four purchases without a legitimate business purpose. The transactions were identified by the Purchasing Department and the money was reimbursed to the University by the cardholder.

Recommendation:
The Department needs to maintain an updated list of Procard cardholders, and perform monthly reconciliations which must be submitted to the supervisor for review. The reconciliations should be signed by both the preparer and the approver.

Level: This finding is considered **Medium** risk because non-business related purchases could go undetected due to lack of timely reconciliation and review by an independent party.

Management Response:
This has been addressed. The Administrative Services Coordinator has been assigned as the Procard Reconciler and Department's Chair as his approver for his Procard. The department does not have any other Procards but will be implementing the policy of the University for any new Procards that may be obtained.

***Responsible Party**:*
Kristen Gonzalez, Administrative Services Coordinator

***Implementation Date:** August 31, 2016*

B.2 Eligibility to Work not Verified Prior to Employment

One employee's eligibility to work was not verified prior to employment. The employee started working at the Geological Sciences Department before the Human Resources Department was notified, and before the required background check was completed.

The completion of the Form I-9 and background check were completed five and twelve business days after the employee's starting date of employment, respectively. This is in violation of the Department of Homeland Security U.S. Immigration and Naturalization Service's regulations, which requires that *"Newly hired employees must complete and sign Section I of Form 1-9 no later than the first day of employment."*

Recommendation:
Work eligibility should be verified before the employee starts working. Guidance should be provided to all departmental employees regarding the completion of Form I-9, new hire paperwork and the timely submission of documents to Human Resources.

Level: This finding is considered **High** risk, due to the possibility that the institution can incur civil fines and criminal penalties for failing to comply with the Department of Homeland Security, Form I-9 requirements.

Management Response:
This has been addressed. The Graduate Coordinator will be responsible for notifying students in advance of their paperwork needs to be submitted prior to them starting work. She will also be implementing a mandatory New Student Orientation before classes begin to distribute the required paperwork. She will be working with administrative personnel to ensure the paperwork is completed properly. The policies and procedures will also be included in the Department's overall goals and objectives.

Responsible Party:
Kristen Gonzalez, Administrative Services Coordinator

Implementation Date: *August 31, 2016*

B.3 Account Reconciliation

The UTEP Handbook of Operating Procedures (HOOP) Cost Center/Project Review Policy Section VII, Chapter 5 (Updated July 30, 2015) states "All cost center/project administrators are required to review the cost center/project for which they have signature authority on a monthly basis.... Discrepancies should be resolved within 60 days after their identification.... Both the reviewer and approver must sign off on the reconciliation. Documentation should be retained and kept available to serve as back up for charges made on departmental accounts." In addition, account reconciliations can identify errors and potential fraudulent activities on a timely basis.

Departmental monthly account reconciliations were not consistently prepared, reviewed and signed-off as required by University policies and procedures.

Recommendation:
Account reconciliation should be prepared on a monthly basis to ensure accurate departmental financial reporting and security of monetary accounts. Both the reviewer and approver must sign-off on the reconciliation. Documentation should be retained and kept available to serve as back-up for charges made on department accounts. Discrepancies should be resolved within 60 days after their identification. In addition, we recommend the cross-training of staff to enhance team performance and organizational success.

Level: This finding is considered **Medium** risk due to the fact that errors and possible fraudulent activities may go undetected because of a lack of timely reconciliation of accounts.

Management Response:
This has been addressed. The reconciler and Chair meet once a month to review reconciliation reports and certifications. The policy and procedures for this will be written with the overall Department goals and procedures.

Responsible Party:
Kristen Gonzalez, Administrative Services Coordinator

Implementation Date: August 31, 2016

B.4 Cash Handling

Employees in the Geology Department receive cash donations for fund raising events. Every year in March, the Department sponsors an event where funds, in the form of cash or checks, are collected from donors. The funds are received, reconciled and deposited by personnel in the department.

According to the HOOP Section IV: Research and Sponsored Projects -Grants, Contracts, and Gifts- Chapter 1 (Updated: March 30, 2015):

> *"1.1.2.2 Proposals for gifts must be forwarded to the Office of Institutional Advancement for review and subsequent approval by the President, or the President's designee, prior to submission to any potential donor. Acceptance of any resulting gifts must be processed by/ through the Office of Institutional Advancement and will be administered by the appropriate University department, office or program in restricted gift accounts as determined by the Office of Institutional Advancement."*

Recommendation:
Donors contributing funds to the Geological Sciences Department should be directed to the Office of Institutional Advancement (OIA). Cash handling policies should be made available to all employees and the segregation of duties for the collection, reconciliation and depositing of funds should be documented.

Level: This finding is considered **Medium** risk**,** due to the fact that donor's funds might not be properly processed in accordance with University guidelines and donor stipulations.

Management Response:
This has been addressed. This will be one of the procedures and policy that is addressed in the overall policies of the Department.

Responsible Party:
Kristen Gonzalez, Administrative Services Coordinator

Implementation Date: *December 31, 2016*

B.5 Travel Reimbursements

According to state travel regulations, a state employee is entitled to reimbursement for the cost of renting a vehicle to conduct state business. The reimbursement may include a charge for loss damage waiver if not already included in the contracted rate for the rental.

For lodging expenses, a state employee may only be reimbursed for his or her actual lodging expense, not to exceed the maximum lodging reimbursement rate.

A sample of three travel vouchers and five travel reimbursements were selected for testing, totaling $15,000.

From the sample selected, we identified the following exceptions:

- One reimbursement included flat tire repairs to a rental car, totaling $285,
- One reimbursement did not include receipts for a hotel expense, totaling $270, and
- One reimbursement included a payment of $8 over the hotel per diem using federal funds.

Recommendation:
The department should ensure personnel have a clear understanding of state travel regulations. Additionally, they should have controls in place to review expense reimbursements before they get approved.

Level: This finding is considered **Medium** risk due to the possibilities of non-compliance with state regulations.

Management Response:
The Department is working on these procedures, a travel form and checklist to better this processing.

Responsible Party:
Kristen Gonzalez, Administrative Services Coordinator

Implementation Date: *August 31, 2016*

B.6 Salaries

We reviewed the paychecks report to identify instances where more than one paycheck was issued to an employee in the same month, and also instances where amounts paid had discrepancies with amounts paid in previous and subsequent months.

We judgmentally selected a sample of nine employees that had one or more instances previously mentioned and requested further explanation and support documentation from the Payroll Department.

Three appointments, four supplemental payments and two changes in contract amounts were processed late due to late submission of information by the Geological Sciences Department to the Human Resources Office. No overpayments were identified; however, off cycle payments had to be requested by department and/or adjustments were made to employees' subsequent paychecks.

Recommendation:
Communicate appropriate deadlines to supervisors to ensure timely submission of payroll data. The department should ensure all appointments or changes on employees' salaries are processed timely to reduce the need for off cycle paychecks or adjustments.

Level: This finding is considered **Medium** risk due to the potential of under or overpaying employees.

Management Response:
We are addressing this by sending email reminders and notifying supervisors in advance of any ending appointments or deadlines. This will be another policy and procedure that is implemented in the overall policies for the Department.

Responsible Party:
Kristen Gonzalez, Administrative Services Coordinator

Implementation Date: *December 31, 2016*

C. IT Security Controls

C.1. Server Backups

In accordance with The University of Texas System Information Resources Use and Security- Policy 165**:** "Standard 6: Backup and Disaster Recovery:

6.1 Backup Plan Requirement.

All U. T. System Data, including Data associated with research, must be backed up in accordance with Risk management decisions implemented by the Data Owner. Each Institution's Backup plan must incorporate Procedures for:

(a) Recovering Data and applications in case of events such as natural disasters, system disk drive failures, espionage, Data entry errors, human error, or system operations errors;
(b) assigning operational responsibility for backing up of all Servers;
(c) scheduling Data Backups and establishing requirements for off-site storage;
(d) securing on-site/off-site storage and Media in transit; and (e) testing Backup and recovery Procedures.

6.2 Disaster Recovery Plan. …

(b) assigning operational responsibility for recovery tasks and communicating step-by-step implementation instructions;"

And the Texas Security Controls Standards Catalog Version 1.3 (TAC 202.76 Security Control Standards Catalog):

"CP-6 Alternate Storage Site
CP4 Contingency Plan Testing
CP-9 Information System Backup"

Backup/restore controls are not being followed or need process improvements to safeguard against loss of data.

- The backups are saved to a server at the same location as the backup source; therefore, there is no copy stored off-site in case the primary site or the disk backup is unavailable.
- There are no written procedures for performing backups or restores for Windows, UNIX, or LINUX servers, which is a risk as there is only one System Administrator.
- Backups must be performed manually by the System Administrator; therefore, backups may not be run if the System Administrator is gone.

- The backup process does not produce any output or log; therefore, no record exists documenting that a backup was performed or if it failed.

Recommendation:
OACS recommends the following:

- *Create a copy of the backup and store it off site, away from the main campus (primary site).*
- *Create written procedures for performing backups or restores for Windows, UNIX, and LINUX servers.*
- *Automate the backup process to avoid human intervention. For example, create scripts and have the operating system schedule and run the script.*
- *Create logs or output when running backups/restores in order to generate records for review or audits.*

Level: This finding is considered **High** risk, due to the fact that data loss can be very costly, impacting critical departmental operations.

Management Response:
As was explained to the auditors previously, the backup issue is a work in progress. All recommendations will be addressed.

Responsible Party:
Carlos Montana, System Administrator

***Implementation Date**: December 31, 2016*

C.2. Contingency Plan for Loss of Key IT Personnel

There is no contingency plan to eliminate the risk of a single point of failure in case of the permanent absence of the System Administrator. When the system administrator is on leave, the generic super administrative passwords are given to the chairperson and a departmental professor.

In addition, there are no policies or procedures requiring the System Administrator to change the passwords for any generic super administrator accounts after his return. A generic super administrator account is an account without a descriptive user value that is able to make any modifications to a server without knowing "who" logged in as the generic administrator (e.g. ROOT, Administrator).

Recommendation:
The Geology Department should have a contingency plan or mitigation for loss of key IT resources such as the System Administrator.

If the generic super administrative account needs to be used, there should be a policy that requires the System Administrator to change the passwords immediately after his return, and keep evidence of the change.

The professor should be set up with a separate account with super administrator rights to use when he is acting as the System Administrator. The account should then be disabled upon the return of the System Administrator.

Level: This finding is considered **High** risk, because personnel knowledge and skills are critical for the operation and maintenance of the systems. Sudden absence of key personnel can negatively affect the department.

Management Response:
An administrator backup operator will be identified for each of our systems. It may not necessarily be the same person for all. For most systems, the root administrator does not need to be shared since group policies or modern Linux policies allow for role based control. For systems that require root account to administer there will be proof of password change.

Responsible Party:
Carlos Montana, System Administrator

Implementation Date: December 31, 2016

C.3. Security Safeguard for PCs

Security safeguard software is not installed in accordance with Texas Security Controls Standards Catalog Version 1.3 (TAC 202.76 Security Control Standards Catalog); therefore, PCs are not fully protected from threats:

> *"CA-7 Security Assessment and Authorization - Continuous Monitoring - A continuous monitoring strategy such as automated and other periodic manual checkpoints is defined*
> *SI-3 Malicious Code Protection*
> *SI-8 Spam Protection*
> *SC-28 Protection of Information at Rest- Information is protected while at rest, through encryption or other security mechanism"*

OACS tested a sample of four PCs from the Chairman's office and found security safeguards missing. The Operating System and Windows updates were current.

Recommendation:
All PC(s) in the Geology Department should be checked for the following security safeguards:

1) disk encryption,
2) anti-virus software,
3) Absolute Management software and
4) Windows current updates, as per UTEP standards.

Level: This finding is considered **High** risk due to the possibility of unprotected computers being exposed to an elevated risk of cybersecurity dangers.

Management Response:
All Geological Sciences departmental office computers will be checked for disk encryption. All other Geological Sciences desktop computers purchased after 2013 will be checked for disk encryption, as outlined by UTEP's ISO. All other Geological Sciences desktop computers older than 2013 will not, as outlined by UTEP's ISO. All Geological Sciences departmental laptops will be checked for disk encryption except the ones that have an exception filed with UTEP's ISO. All Geological Sciences laptops and desktops will be checked for anti-virus, Absolute Management software and operating system updates.

Responsible Party:
Carlos Montana, System Administrator

***Implementation Date**: December 31, 2016*

C.4. Lack of Security Oversight with Information Security Office (ISO)

In accordance with The University of Texas System Information Resources Use and Security Policy 165:

> "1.7. Institutional Information Security Officer (Institutional ISO). The Institutional Information Security Officer is the individual responsible for an Institution's Information Security Program and shall:
>
> *"(a) work in partnership with the University community, constituency groups, and leadership to establish effective and secure processes and information systems and to promote information security as a core Institutional value;*
> *(b) provide information security oversight for all Centralized and Decentralized IT Information Resources; …*
> *(l) perform, at a minimum, an annual vulnerability assessment of Information Resources maintained in both Centralized and Decentralized IT and track implementation of any remediation required as a result of the assessment; "*

And in accordance with the Texas Administrative Code, Title 1, Part 10, Chapter 202, Subchapter C, §202.72 Staff Responsibilities: …

> *"Information Owner Responsibilities. The owner or his or her designated representative(s) are responsible for: …*
> *(D) coordinating data security control requirements with the ISO;*
> *(2) Information Custodian Responsibilities.*
> *(C) adhere to monitoring techniques and procedures, approved by the ISO, for detecting,"*

There is lack of communication and security oversight with the Information Security Office (ISO), which could render the system vulnerable to internal and external threats. The Geology Department stores Category 1 confidential data (e.g. student information) on a

fileserver and the ISO has not been contacted to check the server for security safeguards and vulnerabilities.

Recommendation:
The Geology Department's System Administrator should meet with ISO to review security controls at least yearly. We recommend a completed review by the ISO of the fileserver containing Category I data, and a copy of the results be submitted to OACS.

Level: This finding is considered **High** risk, because Information security policies and procedures at the lowest level of the organization should mirror those at the top of the organization in order to achieve consistency in the management of security issues.

Management Response:
A meeting will be requested with UTEP's ISO. A security audit of the server with Cat 1 data will be requested.

Responsible Party:
Carlos Montana System Administrator

Implementation Date: *December 31, 2016*

C.5. Mission Critical Resources
In accordance with Texas Security Controls Standards Catalog Version 1.3 (TAC 202.76 Security Control Standards Catalog):

> *CP-2 Contingency Plan states:*
> *"a. Develop a contingency plan for the information system that:*
> *1. Identifies essential missions and business functions and associated contingency requirements; …*
> *4. Addresses maintaining essential missions and business functions despite an information system disruption, compromise, or failure…"*

The Geology Department has not documented the information for the identified mission critical resources and computing assets necessary to recover hardware, applications and data in case of a disaster.

> *"Mission Critical Information Resources are defined by an Institution or State agency to be essential to U. T. System or the Institution's ability to meet its instructional, research, patient care, or public service missions. The loss of these resources or inability to restore them in a timely fashion would result in the failure of U. T. System or Institution's operations, inability to comply with regulations or legal obligations, negative legal or financial impact, or endanger the health and safety of faculty, students, staff, and patients."*

Recommendation:
*The Geology Department should d*ocument the mission critical resources with detailed information necessary to recover hardware, applications and data in case of a disaster. The documentation should include the recovery order, as well as the recovery time objective (RTO) and recovery point objective (RPO).

Level: This finding is considered **Medium** risk. Failure or disruption of mission critical factors of a system can result in serious impact on business operations.

Management Response:
Documentation will be prepared to comply with this directive.

Responsible Party:
Carlos Montana, System Administrator

Implementation Date: *December 31, 2016*

C.6. Software for Operating System at "End-of-Life"

In accordance with The University of Texas System Information Resources Use and Security Policy: UTS165:

> "*19.2 Server Hardening. To protect against malicious attack, all Servers on U. T. System networks will be security hardened based on Risk and must be administered according to Policies, Standards, and Procedures prescribed by the Institution, as applicable, and must incorporate Procedures for: … (b) setting baseline security "hardened" configuration Standards for all Servers; and (c) managing the testing and installation of service packs, hot fixes, and security patches.*
> *19.3 Device Configuration. All devices (e.g., routers, laptops, tablets, desktops, and handheld devices) on U. T. System networks must be protected against malicious attack. The Institutional ISO shall establish and communicate security configurations based on Risk and incorporate Procedures for: … (c) recommended patch management practices."*

OACS found that of 18 servers running mission critical systems, three have operating systems which are at or near end of life**.** End of life/support means that the software vendor will no longer provide fixes, security updates, service packs, or online technical support. This could put the server at threat for harmful viruses, spyware, and other malicious software.

Recommendation:
The Geology Department's operating system software should be kept up to date to eliminate the risk of possible threats such as hacking or harmful viruses.

Level: This finding is considered **Medium** risk, due to the fact that Computers which had arrived to the end-of-life do not have support from the vendor, which mean they are left unprotected and vulnerable.

Management Response:
The computing systems with end-of-life status are being phased out, as it was outlined to the auditors.

Responsible Party:
Carlos Montana, System Administrator

***Implementation Date**: December 31, 2016*

CONCLUSION

During the audit, weaknesses were identified which we believe can be strengthened by implementing the recommendations detailed in this report.

We wish to thank the Geological Sciences Department for the assistance and cooperation provided throughout the audit.