Missouri State UNIVERSITY

Audit Follow-Up

February 14, 2022

Report No. 173-22

Office of Internal Audit & Risk Management

DATE: February 14, 2022

TO: Kyle Moats, Director of Athletics
Casey Hunt, Senior Associate Director of Athletics/SWA
Alex Hirdler, Assistant Director of Athletics Compliance
Jeff Coiner, Chief Information Officer
Rob Martin, Information Security Officer
Michael Wills, Director of Procurement
Steve Foucart, Chief Financial Officer
Isaac Balasundaram, Senior Procurement Card Coordinator

CC: Rachael Dockery, General Counsel
Clifton M. Smart III, University President

FROM: Natalie B. McNish, Director, Internal Audit and Risk Management

Audit Follow-Up Report

BACKGROUND

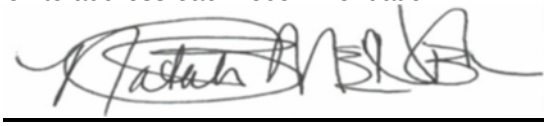
The Office of Internal Audit and Risk Management has completed review procedures to follow up on four audit reports issued between September 30, 2019 and December 31, 2020, to formally report on actions taken by University management in response to audit recommendations.

We interviewed responsible parties and when applicable, requested documentation to determine and support the status of each recommendation. The title and date issued for each of the four audit reports is listed along with a summary of each finding, the recommendation, and the status of the recommendation. The status is classified as one of the following:

> **Implemented**: Management fully implemented the recommendation, either as originally described in the audit report or in a manner that resolved the issue.
>
> **In Progress**: Management has begun to implement the recommendation and intends to complete the implementation process.
>
> **Not Implemented:** Management has not taken action to implement the recommendation.

SUMMARY

These four audit reports included 27 recommendations of which our office is honored to report that all 27 recommendations have been implemented. The Office of Internal Audit and Risk Management applauds University management on the action taken to address each recommendation.



Natalie B. McNish, CFE, CGAP
Director

Grant Jones
Internal Auditor

Audit Field Work Completed: January 28, 2022

Table of Contents

Summaries, Recommendations and Statuses

NCAA Compliance – Financial Aid
September 30, 2019

A compliance audit was completed to review the policies and procedures used to administer and monitor the awarding of financial aid to student-athletes in accordance with NCAA regulation. The scope of the audit included the financial aid awards for the academic years 2016-17 and 2017-18. Additionally, some issues came to our attention for the 2018-19 academic year resulting in a limited review of certain areas during this year.

The bylaws governing a student-athlete's financial aid allow a student-athlete to receive financial aid from the university or from sources outside the institution. The institutional financial aid could include those funds based upon the athlete's athletic ability, the athlete's financial aid need, or other programs administered by the institution. The maximum financial aid a student-athlete can receive is the amount of the institution's cost of attendance. The cost of attendance is an amount calculated by the financial aid office in accordance with federal regulations that includes the total cost of tuition and fees, room and board, books and supplies, transportation and other expenses related to the attendance at the institution. An athlete must receive a written statement indicating the amount, duration, and condition of the award. All athletic financial aid is awarded only for one year.

From October 2018 to July 2019, the university was without a dedicated compliance officer and the duties for this position had been assumed by the Senior Associate Athletics Director/SWA. In July of 2019, Athletics hired a new Assistant Director of Athletics Compliance. To further improve institutional control and compliance, Athletics has implemented a web-based software called ARMS, which automates many processes, provides convenient dashboards and tools for data, and stores necessary documentation to ensure compliance with many requirements.

1. Financial Aid Agreements

For academic years 2016-17 and 2017-18, the University awarded financial aid to 369 and 363 student-athletes, respectively. Review of financial aid agreements for 25 student-athletes revealed that several agreements were not properly signed by the Director of Financial Aid, Head Coach, and Director of Athletics, were signed after deadlines set forth by NCAA Bylaw 15.3, or had no signature. One student-athlete was paid $817 less than the amount on their financial aid agreement. Also, the review identified 13 instances totaling $20,197 where student-athletes received financial aid in excess of the amount stated on their financial aid agreement.

Amended financial aid agreements were not prepared for the situations noted above. Preparing amended financial aid agreements that are signed by the student and the appropriate University personnel is best practices to document a change in the financial aid awarded to the student-athlete. Increasing student-athlete financial aid must be monitored for budgetary purposes and to ensure the sports remain within their equivalency limits outlined in the NCAA Bylaws.

Recommendations:

A. Ensure all financial aid agreements are signed by the required parties by the specific dates on the financial aid agreements and bylaws.

B. Monitor all student-athlete financial aid payments to prevent future underpayments.

C. Issue amended financial aid agreements when the terms of the financial aid is increased so there is adequate documentation of the financial aid provided to each student-athlete, and show that financial aid is properly monitored.

Status:

A. Implemented – At the time of the 2019 audit, the Financial Aid Agreement stipulated a specific timeframe in which the agreement must be signed unique to each sport. After the audit, this document was updated and the timeframe information was deleted. Therefore, the current criteria for timeliness is Bylaw 13.9.3.1 which states, "An institutional or conference financial aid form may be included in the normal mailing of the National Letter of Intent, but none of the forms enclosed in the mailing may be signed by the prospective student-athlete prior to the initial signing date in that sport in the National Letter of Intent program." To review compliance with this Bylaw, we selected 25 student-athletes from all sports for the 2020-21 academic year and determined all agreements were signed in accordance with NCAA Bylaw 13.9.3.1.

B. Implemented – The Office of Athletic Compliance has established periodic reviews of student-athlete accounts to ensure financial aid awards are properly applied. To ensure the effectiveness of this procedure, we reviewed awards applied to the accounts of 25 student-athletes from all sports during the 2020-21 academic year and found no underpayments.

C. Implemented – According to the Assistant Director of Athletic Compliance, new financial aid agreements are completed and retained for any change to a student-athlete's original scholarship. To review the effectiveness of this procedure, we reviewed scholarship documentation for 25 student-athletes from all sports and found no issues with financial aid agreements or amounts.

2. NCAA Squad List Reporting

Squad lists submitted to the NCAA for Baseball, Men's Soccer and Women's Soccer contained errors for the 2016-2017 and 2017-2018 years, including unreported cost of attendance expenses other than tuition/fees, room/board, and books. These unreported "other expenses" resulted in cost of attendance being understated by approximately $4,000 for some student-athletes. Additionally, there was inconsistency in the use of actual cost of attendance or average cost of attendance in equivalency calculations, as well as incorrect reporting of student-athletes' living arrangements, which also impacted cost of attendance reporting.

Recommendation: Ensure data reported on the NCAA squad lists are accurate.

Status: Implemented – The Office of Athletic Compliance now utilizes ARMS Software to generate squad lists and import data directly from Banner to reduce entry errors. Squad lists are generated by the system at a minimum of once per semester. To assess the effectiveness of this new procedure, we verified the cost of attendance values in ARMS matched the cost of attendance values provided by the Office of Financial Aid after they were adjusted for bylaw calculation requirements. No discrepancies were noted in this review.

3. Managing Meal Benefits

Improvement was needed in the management of meal benefits. The former Athletic Compliance Officer failed to communicate the purchase of meal plans for the Men's Basketball team to financial aid personnel. This resulted in student-athlete's financial award accounts being understated. Additionally, there were duplicate payments for the meal plans of the Men's Basketball team for the 2018-2019 academic year which necessitated the update of financial awards and, in at least one instance, a student-athlete was required to return their overpayment to ensure that their financial aid award did not exceed cost of attendance.

Meal benefits must be included in each student-athlete's financial aid award to ensure NCAA violations for over awards do not occur. Although NCAA violations did not ultimately result from these two issues, the potential existed for a violation because all student awards for Men's Basketball were not properly monitored.

Recommendation: Develop procedures to properly monitor meal benefits and ensure they are properly included on each student-athlete's financial aid award account.

Status: Implemented – According to the Assistant Director of Athletics for Compliance, athletics has improved communication with the Office of Student Financial Aid to ensure meal benefits are accurately included in the student-athlete's financial aid award. To assess the effectiveness of this change, we reviewed awards given to 25 student-athletes from all sports and determined all meal benefits were appropriate and included in the financial aid award.

4. Men's and Women's Basketball

During the Spring 2018 semester, a Women's Basketball student-athlete received aid totaling $4,900 but no financial aid agreement could be located. NCAA Bylaw 15.3 requires that each student-athlete receives a written financial aid award statement. The financial aid provided to the student-athlete was also not included in the 2017-2018 squad list reported to the NCAA in accordance with Bylaw 15.5.11. Additionally, this same student-athlete received $1,230 in athletic aid to live in on-campus housing over the Summer 2018 semester; however, this student-athlete never registered or attended classes. NCAA Bylaw 15.2.8 allows student-athletes to receive summer financial aid provided the student is attending summer term.

A Men's Basketball student-athlete, who received a $750 University Dean's scholarship, did not have their athletic financial aid reduced by this amount to ensure their total financial aid did not exceed the cost of attendance. Instead, the $750 was refunded to the student-athlete in error, resulting in the student-athlete receiving awards totaling $77 in excess of the Cost of Attendance during the 2016-2017 academic year. NCAA Bylaw 15.1 limits the total value of all financial aid awards to the Cost of Attendance.

Recommendation: Improve student-athlete financial aid monitoring to prevent future violations.

Status: Implemented – The violations were self-reported to the NCAA after bringing these matters to the attention of athletic administration. According to the Assistant Director of Athletics Compliance, athletics periodically reviews student-athlete accounts to ensure financial aid awards are properly awarded. To assess the effectiveness of this procedure, we reviewed student accounts and awards given to 25 student-athletes representing all sports and determined no instances of non-compliance were noted.

5. Cost of Attendance Calculations

NCAA Bylaw 15.02.2 indicates that the cost of attendance is an amount calculated by the institution's Financial Aid Office. Our review noted that both the Athletic Department and the Financial Aid Office calculated the University's annual cost of attendance. Consequently, the amounts these two departments calculated differ slightly each year. The Athletic Department should use the cost of attendance data reported by the Financial Aid Office as stated in the NCAA Bylaw.

Recommendation: Utilize the cost of attendance data reported by the Financial Aid Office

Status: Implemented - The Office of Athletic Compliance developed procedures to request cost of attendance data, with breakdowns for each element of cost of attendance, at the conclusion of the preceding academic year from the Financial Aid Office. We verified the cost of attendance values in ARMS matched the cost of attendance values provided by the Office of Financial Aid after they were adjusted for bylaw calculation requirements.

6. Improve Institutional Control

Institutional control over NCAA compliance should be improved. The Athletics Department was without a Compliance Officer between October 2018 and July 2019, during which time these duties were temporarily assumed by the Senior Associate Athletics Director/SWA. Supervision of the Compliance Officer that was employed prior to October 2018 was noted as lacking, which resulted in some of the deficiencies noted in the report. Ensuring complete and accurate financial aid agreements, accurately reporting squad list data

to the NCAA, tracking student-athlete living arrangements, and working with University financial aid personnel to manage meal benefits and other aid are just a few of the routine controls that should be in place to maintain adequate institutional control.

Recommendation: Take steps to improve institutional control over NCAA financial aid compliance.

Status: Implemented – Since the hiring of the new Assistant Director of Athletics Compliance, athletics has implemented a new system of compliance tracking (ARMS), spearheaded rules education with the Financial Aid Office, and has developed several new processes that reduce errors in applying or awarding athletic aid. Based upon our review of other items noted in this follow-up, institutional control over financial aid compliance has much improved since the 2019 audit and we commend the Athletics Compliance staff for their work to advance the University's compliance focus.

Distributed Servers
September 30, 2019

The Division of Information Services is a centralized asset composed of various information technology (IT) personnel who assist with the development, installation and user support functions of information services needed to secure and maintain various administrative and educational operations the University. As the University has increased its use of technology over time, individual colleges and units have wanted dedicated IT personnel to increase response time and expedite technology implementation. From this desire for dedicated service, distributed system personnel were hired to develop distributed IT systems, including servers. These personnel are supervised by their individual colleges and units and charged with the development and management of IT assets not provided by Division of Information Services. In addition, during the Cybersecurity Risk Assessment completed in April 2018, it was noted management should take a closer look at potential risks existing in the distributed environment.

Our office reviewed distributed services to determine the sufficiency of established controls in place during the fiscal year ending June 30, 2019.

1. Control Environment

Improvement of the control environment for distributed systems was necessary. An organization's control environment is the foundation for all other control activities. It includes the attitudes, awareness and actions of management, the governance policies and organizational structures, and the overall mission, values and principles that set the tone for the implementation and achievement of strategic objectives.

A. Organizational Structure

The University's overall information technology environment could be strengthened by joining the distributed and centralized personnel through a dotted-line or secondary solid-line relationship within the organizational structure.

Distributed personnel have unique and specialized knowledge of their units and the roles played by distributed systems. Using the varying structures, resources, and tasks confronted, each has built a system which serves the direct educational and support needs of their unit. Some have pioneered differing or new methodologies successfully, and through those challenges, have built knowledge which can benefit the entire University. Likewise, the Division of Information Services has its own unique and specialized knowledge of centralized systems, risks, and resources. This unit is charged with the responsibility of ensuring all University information system needs are met in the most secure manner possible.

By adding an organizational relationship between the distributed and centralized systems, both environments could benefit from shared knowledge, resources, advancements, and challenges.

B. Policy

The Division of Information Services had not established a policy specifically addressing distributed systems and most existing operating policies are not clear as to their application in the distributed environment. The purpose and structure of each distributed system is unique to its own environment and some of that uniqueness may be crucial to its operation; however, there are many areas in which policy would add value to these systems. Criteria for allowing a system to be distributed in nature, criteria for allowing the system to be housed outside of a data center, and identified physical and informational security requirements would provide a foundation for these systems. In addition, these policies should provide the Division with oversight of the machines operating on the University's network.

Recommendations:

A. Consider establishing an organizational relationship with distributed staff.

B. Revise current and/or develop new policies that address risks within the distributed environments.

Status:

A. Implemented – Management considered a more direct organizational relationship between distributed and centralized support personnel but decided that instead of an organization structure change, the purpose of this recommendation could be achieved through increased and improved communication. To improve communication, the Division of Information Services includes distributed support personnel in meetings that occur weekly and monthly to help facilitate the sharing of information and improve collaboration between the two environments.

B. Implemented – The Division of Information Services and the Distributed Server Audit Response Task Force developed the University Servers Policy (Op12.07-18), which was adopted on September 21, 2020. This policy requires every server to have a named Server Administrator who is responsible for maintaining information about the server in the University Server Registry, configuring the server's operating system and software to prevent security weaknesses, installing security updates on a timely basis, addressing issues identified in periodic vulnerability and configuration assessments, ensuring the physical security of the server, completing an annual risk assessment form, and providing the Information Security Office with a Disaster Recovery Plan that addresses timely service restoration in the event of a disaster or incident.

2. Physical & Virtual Security

Physical security of distributed environment assets is critical to the functionality of both the distributed and centralized systems. Our audit determined physical security controls could be improved. In addition, the distributed environment appeared to be moving in the direction of virtualization and while this offers many benefits to these distributed environments, it also presents a host of risks. Our audit determined there is low/no oversight of these virtual machines (VMs) by the Division of Information Services.

A. List of Distributed Servers

The list of distributed servers maintained by the Division of Information Services was incomplete, sometimes inaccurate, and the application used to maintain the list was cumbersome for users. The Division had developed an application which tracks distributed servers on the University network. This list provides a place for server name, location, college or unit served, department head, system administrators/primary technicians, server make/model/type and serial number,

current operating system, purpose, data sensitivity, and an audit log showing when the information was last updated and by whom.

A review of the information held on this list and discussions with the distributed staff determined distributed system staff did not feel they clearly understood what assets and information were required and were often unable to view or change information recorded by a different user, some vital information such as host machine identification or indication of active/inactive was not recorded, at least 20 active servers were not included on the lists and at least 8 servers listed as active were actually test environments or inactive. In addition, two servers listed were claimed to be personal assets and quite a bit of the information recorded was incomplete or out-of-date.

A complete and accurate list of all assets connected to the University network is necessary to ensure both the accountability and security of University assets. In addition, the Division should establish procedures to review the information reported and investigate inaccuracies, risks, and other issues such as the personal assets noted above.

B. Physical Safety

Physical controls for many distributed servers are not sufficient. University operating policy 12.07-5 Physical Security, requires, "facilities that house data systems and data storage, workstations, and other computing devices will be protected from unauthorized physical access, as well as natural and environmental threats that may compromise confidentiality, integrity, or availability." For a physical machine to be considered secure, minimum controls in place should include:

- Physical access to servers should be restricted to authorized users only.
- Protection from electrical system surges and failures should be provided.
- The environment should be heat and humidity controlled.
- Storage areas should be free from water intrusion or leakage.
- Fire suppression mechanisms, such as fire extinguishers rated for electronic equipment, should be installed in close proximity.

During our review of physical controls in various distributed environments, we determined several services were not in compliance with these five minimum controls.

Physical controls for many of these distributed servers could be improved by relocating the physical machine to the data centers established in Cheek or Blair-Shannon Halls. These data centers were constructed to meet all physical control standards and have capacity to house more machines than currently exist. When discussing this option with various distributed system staff, several barriers were identified. Barriers included: the need for physical access to certain machines based upon configuration or maintenance requirements, the contractual requirements to maintain all assets on one local network, the use of non-rackable machines, and the increased costs charged by the University's Office of Networking and Telecommunications for use of these data centers.

C. Virtual machines

The Division of Information Services should provide oversight or guidance regarding the use of virtual machines (VM). VMs are computer software developed to function as a separate system within the system they are installed (hosted). Each host can provide the foundation for several VMs. This technology has several benefits, including lower costs and greater flexibility; however, it also comes with unique risks which require additional oversight. The Cloud Security Alliance released a whitepaper titled "Best Practices for Mitigating Risk in Virtualized Environments" in April 2015. This whitepaper noted 11 significant risks found in the virtualized environment.

As physical servers are meeting their end of useful life, many areas are looking toward virtualization as a cost-effective replacement. Without direct guidance establishing basic controls, it is probable security risks could exist without the Division's knowledge.

Recommendations:

A. Information Services will collaborate with distributed IT staff and IT Council to maintain a complete inventory of distributed servers. Information Services will make improvements to the distributed server inventory application to improve usability and data collection.

B. Information Services will work with the distributed IT staff and IT Council to address barriers that prevent physical machines from being housed in the University's data centers and to develop minimum physical controls standards.

C. Information Services will work with the distributed IT staff and IT Council to develop server configuration standards for virtual machines.

Status:

A. Implemented – A collaborative effort between the Division of Information Services and the Distributed Server Audit Response Task Force resulted in the development of the University Server Registry within the University's existing Information Technology Service Management (ITSM) application, TeamDynamix. All servers on campus are required to be entered into this registry.

B. Implemented – The Division of Information Services and the Distributed Server Audit Response Task Force worked together to identify and remove barriers that prevented distributed servers from being hosted in the central data center, including providing physical access to the central data center for distributed server administrators and establishing the Missouri State Private Cloud, which provides hosting for virtual servers in the central data center. Additionally, the Division of Information Services and the Distributed Server Audit Response Task Force established physical security standards for distributed servers that are housed outside of the central data center that are line with the existing Physical Security Policy (Op12.07-5).

C. Implemented – The Division of Information Services and Distributed Server Audit Response Task Force established secure configuration standards for servers and pre-built virtual server templates that meet industry standards.

3. Informational Security

Security of the information stored on distributed servers was at risk due to a lack of vulnerability assessments performed, tested offsite backups of some systems, lack of documented disaster recovery plans, use of unsupported or under supported operating systems, and incomplete controls over virtual machines.

A. Vulnerability Assessments

Most distributed servers were not scanned for vulnerabilities on a scheduled basis. The Information Security Unit has various tools to scan servers for certain vulnerabilities, such as misconfiguration, defect, or error in an operating system. We asked the Division of Information Services to complete scans of 2 servers selected based upon risk assessments. One server appeared to be well protected; however, the other server was misconfigured and access to folders containing restricted information was allowed to more users than necessary.

B. Backups & Disaster Recovery Plans

Procedures to backup electronic data stored on distributed machines were in need of improvement, and formal documented disaster recovery plans for each distributed environment did not exist. We determined many machines were not being backed up at all, and some which were being backed

up were not storing backups off-site or testing the data to ensure it is complete and reliable. Further, we noted none of the distributed environments had documented disaster recovery plans.

Backing up electronic data safeguards the University against viruses, equipment failure, physical damage to machines and theft. Failure to backup electronic data could cause significant interruptions in the learning environment or with the business operations of the University. Operating policy 12.07-12 requires, "Each department with separate information systems is responsible for developing and maintaining their own disaster recovery plan in consultation with the Information Security unit of Information Services."

C. Unsupported/Under Supported Operating Systems

Some distributed servers were running unsupported, under supported, or soon to be unsupported operating systems (OS). The OS is software installed on a device to manage all other associated hardware and software installed and facilitate various processes to ensure each portion of the system operates as it should. The developer of each OS determines how long general support and technical guidance will be provided. During the phase of general support, the developer provides access to new and existing maintenance updates/upgrades, security patches, bug fixes, etc. However, at the end of this phase, the developer is no longer making new updates, upgrades, patches, or fixes to help the OS battle new problems. As a result, security risks begin to surface, and the OS runs less effectively and is no longer as effective at protecting the user or the data stored on the device. With the ever-changing threat of cybersecurity, running unsupported OS creates a significant risk to University systems and data.

D. Testing environments

Network isolation was not always used in distributed testing environments. Testing environments are used by various distributed personnel to develop, test, and refine software applications needed for their operations. During the testing phase, the distributed personnel install and begin processing information in the application to determine its functionality, limitations, and methods to assist users in its use. At the time of installation, distributed personnel may not know the vulnerabilities existing within the software application and therefore, use of network isolation is critical to the protection of all other assets. This allows vulnerabilities to be addressed while protecting other information assets.

Recommendations:

A. Complete vulnerability assessments of distributed machines on a periodic basis. The Division should communicate all risks identified and ensure corrections are made to safeguard university assets.

B. Work with distributed environment staff to remove barriers related to backups, ensure backups are completed on a scheduled basis, ensure backups are tested and stored off-site, and require formal documented disaster recovery plans to be filed with the Information Security Unit.

C. Require all machines to update to a supported operating system. If it is determined a machine cannot be updated, the Division should take steps to isolate these machines from the rest of the University network.

D. Require network isolation be established for testing environments.

Status:

A. Implemented - The Information Security Office now completes quarterly vulnerability scans for all University servers and communicates those results to server administrators. Servers that have been identified as high risk receive more frequent scans.

B. Implemented – The Division of Information Services now offers distributed services the ability to utilize the University's approved cloud environment for backup services and requires all distributed systems to submit a disaster recovery plan. As of January 2022, all distributed systems except one (which experienced delay due to staff turnover) have complied. The Information Security Office is working with the remaining unit to finish their plan as soon possible.

C. Implemented – The Information Security Office now requires all servers run a supported operating system and that operating system security updates be regularly installed. If university business needs require that the server run an unsupported operating system, network isolation is utilized to mitigate the risk.

D. Implemented – The Information Security Office published secure configuration guidance, which requires new test servers to be placed in an isolated network segment.

Review of Vending Machine Services Contract
February 19, 2020

Prior to 2005, the University owned and maintained all food vending machines on the Springfield campus (with the beverage machines outsourced to Pepsi Americas). During 2003 and 2004, the University averaged only $8,000 net profit on average sales of $446,875 per year so a decision was made to also outsource the food vending machines. A six-year contract running from January 1, 2005 through December 31, 2011 was awarded to Canteen Vending. They would use the University-owned machines and, in addition to paying a $100,000 up front bonus, would pay commissions of 20% on gross sales with a yearly guaranteed minimum of $75,000. Unfortunately, vending sales were not as high as Canteen had anticipated so the University received only the $75,000 minimum payment each year of the contract. Over the initial period, the contract was assumed by Burch Food Services, and then by Jackson Brothers.

A new five-year contract effective January 1, 2012 was awarded to Jackson Brothers with renewal options extending through December 31, 2021. Terms of the new contract provided commissions of 22% on gross sales with a guaranteed minimum of $31,000 per year. In addition, Jackson Brothers purchased all remaining University-owned machines for $53,300.

Our office completed this audit to determine compliance with the contract terms and accuracy of commissions paid. The scope of this review included, but was not necessarily limited to, calendar years 2016 through 2019.

1. Commissions

While the Office of Procurement received a copy of the commission report monthly, no one from the University compared the report to commissions paid or other details of the contract to monitor compliance. As a result, commission calculation methodology was inconsistent or inaccurate, reporting was not sufficiently detailed to monitor contract compliance, and overall, it was determined Jackson Brothers underpaid commission totaling $4,385 for the period of July through November 2019.

A. According to the vending machine services contract, commissions paid to the University should be calculated on gross sales, including sales taxes. However, commission checks received from January 2012 through October 2017 had a note typed on them stating sales tax was deducted prior to the calculation of commissions. Auditors attempted to recalculate the sales and sales tax to confirm the value of commissions paid, but Jackson Brothers could not provide detailed sales reports. The Senior Vice President of Jackson Brothers explained that even though detailed sales reports were not available, meter readings from machines could be used to calculate sales; however, auditors found these meter readings were also not reliable. Jackson Brothers

management also explained that the commissions were not based upon sales but were based upon the amount of money turned in from each machine. This methodology does not comply with the contractual terms.

In June 2019, Jackson Brothers began using new vending software that provided more detailed reporting. Auditors reviewed commission calculations from June to September 2019, and determined sales taxes were improperly deducted to calculate commission and 12 campus vending machines were not included on the commission report resulting in an underpayment to the University of $4,385 for the four month period.

B. According to Jackson Brother's representatives, the new vending software would more accurately track sales and meter readings. To determine the accuracy of the prior procedure and reporting mechanism used by the contractor, auditors calculated sales based upon machine meter readings for July through November 2019 which totaled $81,559. Comparing this amount to the $78,099 gross sales (based on cash collections) reported on the commission reports indicated a $3,460 cash shortage occurring over the five-month period. This discrepancy proved the prior period reports received were likely inaccurate and identifies that the University's commission loss may be greater due to lack of contract revenue monitoring.

Recommendations:

A. Procurement Services should request and receive detailed sales reports as required by contract terms and periodically review the calculation of commissions paid to the University for accuracy.

B. Procurement Services should request Jackson Brothers to calculate sales based upon vending machine meter readings to verify the accuracy of sales amounts used to calculate commissions.

Status:

A. Implemented – As initially reported, Jackson Brothers remitted the $4,385 commission shortage in October 2019. Since then, Procurement Services has developed procedures to forward monthly reports that detail sales for each machine as well as the commission generated by each machine to Financial Services for review and reconciliation to commission checks received.

B. Implemented – The monthly report that Procurement Services now receives includes meter readings calculations as well as gross sales calculations. Meter readings still vary significantly from gross sales due to meter entry/transmission errors; however, commission amount is being calculated based upon gross sales, per the existing contract with Jackson Brothers.

2. eFactory Micro Market

In February 2018, a micro market was installed at the eFactory by Jackson Brothers. Micro markets have the appearance of an unattended mini convenience store where customers select items from open shelves and coolers, then use a self-checkout scanner to pay with a credit card. When the micro market was originally installed, the eFactory had a network jack installed for processing these transactions. This left the University vulnerable to potential PCI DSS compliance violations, which could result in severe penalties and fines. After installation was complete, the beverage machines operated by Ozarks Coca-Cola were removed. The University has a contract with Ozarks Coca-Cola that provides them exclusive rights to all beverage sales (soft drinks, juice, bottled water) on campus and allowing Jackson Brothers to sell these products violates that exclusivity. In addition, the University receives significantly less commission on the sale of these products through Jackson Brothers than it does from machines operated by Ozarks Coca-Cola, which created a conflict of interest in these transactions.

A contract modification for both Jackson Brothers and Ozarks Coca-Cola was needed if the micro market concept was going to continue on-campus. The loss of beverage commissions should be considered when modifying contract terms.

Recommendation: Procurement Services should have participated in setting up the micro market to ensure contract terms and University policy were followed. If micro markets are going to continue or increase on campus, contract addendums should be put in place that would ensure the University receives an appropriate amount of commissions and conflicts of interests are avoided.

Status: Implemented – The Jackson Brothers contract amendment from April of 2020 stipulated that they must utilize cellular data transmission service for their credit card payments at the eFactory Micro Market and that their point-of-sale software is appropriately reviewed by a third-party company and is PCI compliant and clarified the sale of beverages and applicable commissions.

3. Product and Pricing Issues

The vending machine services contract indicated the University had the right to select the types of products sold and required the University to approve product pricing. While the contractor had submitted price increase requests for the list of products included in the 2012 original contract, the audit identified additional items being sold or fees charged which had never been submitted to the University for approval. For example, auditors found office supplies being sold in the library, identified some vending machines were charging an additional fee when customers paid with a debit/credit card, and noted the eFactory Micro Market was selling Coca-Cola products at higher prices than machines operated by Ozarks Coca-Cola, and all without University approval.

Recommendation: Procurement Services should meet with the Jackson Brothers representatives and remind them of the scope of items allowed to be sold under their contract. If the University approves of them selling Coke products at the eFactory Micro Market and office supplies in the Meyer Library, then the contract should be amended to include these items, and prices for these items should be submitted for University approval.

Status: Implemented – The contract amendment signed in April 2020 set prices for Coca-Cola products being sold at the eFactory Micro Market and denied the contractor the ability to sell office supplies in the Meyer Library. Additionally, the contractor ceased charging additional fees for use of credit/debit cards once brought to their attention during the audit process.

4. New Contract

The University's Procurement Office renewed the vending contract with Jackson Brothers in November 2019 for one year. The contract was originally written in 2012 and is outdated in the use of various vending terminology. The contract also did not address PCI compliance for credit card transactions or include an audit clause that reflects the use of electronic data that is currently available.

Recommendation: When renewing the vending contract at the end of 2020, Procurement Services should ensure to update contract terms to reflect current practices.

Status: Implemented – The Office of Procurement signed contract addendum with Jackson Brothers in April of 2020 that addressed the concerns identified in the audit.

Review of Amazon Prime Purchases
August 3, 2020

In January 2019, the University paid $3,499 for an Amazon Prime business membership for all university colleges and departments to have access to a myriad of savings and efficiencies. The Office of Procurement Services estimated that the discounts and free shipping offers would more than make up for the additional cost the University incurred to monitor and guide purchases. Our office reviewed purchases made using

the University's Amazon Prime business membership during calendar year 2019 to determine the benefit offered and risks afforded through this program.

During the year ended December 31, 2019, the University system spent nearly $655,000 with Amazon. According to spending data extracted from the Amazon system, the largest number of orders and dollars spent were for office products (15%), books (14%), hardware and tools (12%), and personal computers (12%). Our review noted the University received discounts totaling $15,833, plus free shipping and other benefits resulting from the 2019 membership.

During the year ended December 31, 2021, The University system spent approximately $835,000 with Amazon. The largest categories of expense were personal computers (12%), books (12%) and personal computer accessories (11%). The University received discounts totaling $27,509, plus free shipping and other benefits resulting from the 2021 membership.

1. Encourage Comparative Pricing

Nearly $100,000 was paid to Amazon for office supplies and copy paper when the University has separate vendor contracts for these items at lower prices. As a result, the University paid more for these items than they should have. In a comparison of selected items purchased, we found an average savings of approximately 30 percent on office supplies when ordered from Office Depot, and an average savings of approximately 50 percent on copy paper when ordered internally from the University's Central Stores.

Operating Policy 8.16, Procurement Procedures, states, "Although solicitation is not required for purchases costing less than $3,000, university staff are encouraged to exercise good judgment to ensure university funds are spent reasonably and responsibly. Governing Policy 1.13, Fiscal Responsibility, further explains that University employees have an "obligation to practice conscious and wise stewardship" of University funds. To encourage fiscal responsibility, Procurement Services should utilize banner notifications within the Amazon Prime system directing employees to University contracts and consider more education of users to encourage price comparisons for items such as office supplies and copy paper before purchasing.

Recommendation: Utilize banner notifications in the Amazon Prime account to encourage users to compare prices of office products before purchasing.

Status: Implemented – A banner was added to all office product categories stating "Please compare prices for office supplies and printer ink to Office Depot. Also, use Central Stores for paper supplies." We reviewed Amazon Prime orders during calendar year 2021 to determine purchase of office products through Amazon Prime has decreased by 31 percent with this additional banner in place.

2. Unallowable Procurement Card Purchases

Users ordered items from Amazon Prime which were specifically identified as unallowable purchases on a university procurement card. Examples include computers, food, furniture and many other items. However, if a purchaser can provide reasonable support for purchasing an unallowable item, a written exception letter may be granted from Procurement Services and the charges are allowed on a university procurement card. Also, some unallowable purchases were not identified by Procurement Services because the procurement card system does not always provide a complete listing of what was purchased from Amazon Prime. These purchases must be viewed through the Amazon Prime system to view the details of what was purchased. Adding a review of the Amazon Prime system purchases would improve the monitoring procedures already established by Procurement Services.

Recommendation: Clarify the list of unallowable procurement card purchases, educate cardholders on these changes and consider developing separate review procedures for Amazon Prime purchases on a periodic basis.

Status: Implemented – The Amazon Prime Business Account webpage has been updated to include a list of restricted categories (which are still purchasable, but have a banner notification reminding the user of

the University's fiscal and P-Card policies) and a list of blocked categories (which cannot be found on searches and direct links to the products will not allow the product to be added to the user's cart). In addition, the Office of Procurement has established procedures to review unallowable purchases on the Amazon Prime Business Account. If the purchase is deemed to be unallowable, a memo is sent to the user to reeducate the user of allowability guidelines.

3. Terminated Users

Procurement Services had not immediately terminated Amazon Prime access for users who are no longer working for the University. The audit found the University had 455 registered users for its Amazon Prime account as of March 12, 2020, and 12 were determined to no longer be employed by the University, including 9 who had been terminated for more than 100 days prior to our review. To ensure the benefits offered by the University's membership are used solely for University purposes, it is important to ensure access to the Amazon Prime membership is terminated immediately upon the resignation or termination of an employee.

Recommendation: Develop procedures to ensure the University's Amazon Prime Business account access is immediately terminated for all employees who are no longer associated with the University.

Status: Implemented – Procurement Services developed procedures to ensure users are removed as soon as possible following termination of employment. To verify the effectiveness of these established procedures, we compared a list of employees who were authorized users and who terminated employment with the University in November 2021 to a current list of authorized users and determined access had been terminated as required.

4. Personal Purchases

The University's Amazon Prime Membership, related benefits and tax exemption had been used to make personal purchases in violation of university policy. During the year ended December 31, 2019, 105 personal orders were placed by 22 different users. Although these purchases were not paid for by the University and totaled only $2,594, these users benefited from the membership through pricing discounts, free shipping and tax exemption. According to University Governing Policy G1.29 Code of Conduct, "University resources must be reserved for business purposes on behalf of the University. They may not be used for personal gain, and may not be used for personal use except in a manner that is incidental, and reasonable in light of the employee's duties."

Recommendation: Ensure violations of the Code of Conduct are reported to the user's direct supervisor and strengthen the information on the Amazon Business Account webpage to directly identify the misuse of the membership as a Code of Conduct violation.

Status: Implemented – The Office of Procurement Services developed procedures to identify personal use of the University's Amazon Prime Membership while reviewing purchases for allowability. These reviews are done in regular intervals and if a personal purchase is identified, a violation memo is sent to the user, the user's supervisor, and the Office of Internal Audit & Risk Management. Further, the Office of Procurement Services made changes to its webpage to directly identify use of this resource by employees for personal gain as a Code of Conduct violation.