Arizona State University
Office of University Audits
Information Technology General Controls
Educational Outreach and Student Services
5/8/2019

This page intentionally left blank

Summary: The Information Technology General Controls audit was included in the Arizona State University (ASU) FY 2019 audit plan approved by the Arizona Board of Regents (ABOR) Audit Committee and ASU senior leadership. The audit focused on the design and effectiveness of controls related to operations, access management, and change management for Educational Outreach and Student Services (EOSS). This audit is in support of ASU's mission of preserving the availability, confidentiality, and integrity of its information resources.

Background: Information technology general controls are controls that apply to all systems, and cover the general areas of access management, change management and computer operations to ensure availability, confidentiality, and integrity of information resources. ASU's Information Security Office has developed and implemented various policies to govern information technology general controls as referenced below:

Access Management: A combination of physical and logical controls that prevent or detect unauthorized use, damage, loss, or unauthorized modifications to information assets.

- Information Security Policy
- Access to University Technology Resources and Services Policy
- Privileged Accounts Standard
- Password Standard

Change Management: Establishes a framework for managing change within the Information Technology environment including ensuring changes are properly authorized, tested, approved, implemented, and documented.

- Enterprise System Change Management Standard

Computer Operations: A combination of controls addressing overall availability, confidentiality, and integrity of information resources including areas such as monitoring and logging, encryption, backup and recovery, patch management, and vulnerability management.

- Data Handling Standard
- Patch Management Standard
- Systems Audit Requirements Standard
- Web Application Security Standard
- Anti Malware Standard
- Network Vulnerability Management Standard

When information systems are managed directly by a college or business unit, they are responsible for ensuring they meet all defined ASU Information Security policies and standards. In addition, if the system is hosted with a third party, the college or business unit retains ownership for ensuring the third party is compliant with defined security

provisions included in the contract, which address general computer controls among other items.

Audit Objective: The objective of this engagement was to assess the design and effectiveness of general computer controls managed within EOSS. Specifically, the following areas were assessed:

- Ensure departmentally managed applications are compliant with policies addressing logical access, password complexity, change management, encryption, logging and monitoring, backup and recovery, patch management, and vulnerability management
- Ensure appropriate oversight controls have been implemented to monitor third party hosted applications for compliance with defined security provisions
- Ensure applications are accurately reflected in the departmental continuity plan
- Identify opportunities for improvement

Scope: The scope of the audit focused on assessing information technology controls for eight high-risk departmental applications managed by EOSS. Applications chosen included applications that contained sensitive information such as student data, HIPAA data, as well as critical applications required to fulfill EOSS business objectives. Control activities performed by the University Technology Office were not considered in scope for this review and therefore were not assessed. For EOSS, all applications were supported by UTO or the third party vendor except for logical access and password complexity. As such, other areas including change management, encryption, logging and monitoring, backup and recovery, patch management and vulnerability management were not considered in scope for this review outside of the third party monitoring activities that should be in place for these areas.

In addition, the Kinderlime application was part of our initial selections. This application is utilized by the Sun Devil Fitness Club for summer camps. The application was purchased without a security review or formal contract in the summer of 2018; however, is currently not being utilized. EOSS is planning to utilize Kinderlime again for 2019 summer camps and communicated that they are currently performing the required security review.

Methodology: Our audit consisted of tests of procedures necessary to provide a reasonable basis for expressing our opinion. Specifically, audit work consisted of interviews with application owners, observation of work processes, review of documented policies and procedures and substantive tests including the following areas:

- For applications managed by ASU, the following procedures were performed:
  - Validating unique user IDs are utilized through review of access listing.
  - Performing a high-level access review based on job title and department and if applicable, confirming training requirements were met.
  - Ensuring privileged access is appropriately restricted.
  - Reviewing password configuration to ensure password complexity requirements have been met.
- Assessing oversight of third party compliance to the defined security provisions through inquiry with the process owner and review of SOC2 reports where available.
- Validating that the continuity of operations plans (COOP) accurately represent the departmental applications.

Conclusion: Overall, some information technology controls have been implemented including security reviews and vendor oversight; however, further improvement is required in the areas of access management and password configuration. It was also noted that the continuity of operations plans lacked accurate application data to ensure recovery.

Specifically, EOSS has implemented effective processes to ensure security reviews are performed as required. Testing indicated that in addition to the minimum requirements, the IT team has also began performing full security reviews on existing applications to ensure appropriate visibility in high risk areas. In addition, EOSS has implemented vendor management oversight processes for third party service providers; however, should continue to enhance the associated documentation to support their oversight activities.

Testing also indicated that logical access is not appropriately restricted. Specifically, inappropriate user access was noted in six of the seven applications reviewed with exception rates ranging from 4% - 12%. Four of the applications also utilized generic accounts. At the time of this review, EOSS was in the process of implementing single sign on (SSO) for one of these applications, which will eliminate the use of generic accounts; however, had not yet completed this change. In addition, there were multiple exceptions noted where existing password configuration for local accounts and applications not utilizing SSO did not meet the defined Password Standard.

The control standards University Audit considered during this audit and the status of the related control environment are provided in the following table.

General Control Standard (The bulleted items are internal control objectives that apply to the general control standards, and will differ for each audit.)	**Control Environment**	**Finding No.**	**Page No.**
Reliability and Integrity of Financial and Operational Information	Not Applicable	N/A	N/A
Effectiveness and Efficiency of Operations	Not Applicable	N/A	N/A
Safeguarding of Assets			
• Logical access to the departmental applications is appropriately restricted.	Opportunity for Improvement	1	6
• Password requirements and complexity configuration meet the defined Information Security Policy.	Opportunity for Improvement	2	7
• Security reviews are in place to ensure technology purchases comply with ASU's Security Review requirements.	Reasonable to Strong Controls in Place	N/A	N/A
• Third party vendor management oversight is implemented to ensure compliance with defined Security provisions.	Reasonable to Strong Controls in Place	N/A	N/A
• Departmental applications are accurately reflected in the Continuity of Operations Plans.	Opportunity for Improvement	3	8
Compliance with Laws and Regulations	Not Applicable	N/A	N/A

We appreciate the assistance of the EOSS staff during the audit.

Lisa Grace, Executive Director, University Audit and Advisory Services
David Jones, IT Auditor Senior, University Audit and Advisory Services

1. Logical access to departmental applications is not appropriately restricted.

Condition: Logical access to departmental applications is not appropriately restricted. Specifically, inappropriate user access was noted in six of the seven applications reviewed. Exception rates of inappropriate access ranged from 4% - 12%, in one instance the full population was not tested due to the high exception rate. In addition, generic accounts were in use in four of the applications.

Criteria: ASU's Access to University Technology Resources Standard limits access to ASU technology resources to a unique ASURITE ID, provisioned based on affiliation status and access should only be granted to active affiliate IDs that are authorized as required by ACD 125: Computer, Internet, and Electronic communications Information Management Policy.

Cause: Application owners are responsible for granting/removing access to departmental applications; however, formalized provisioning processes are not in place. As a result, they are dependent on departments notifying them when access should be removed. Consistent notification processes are not in place, as a result, the application owner is not always notified when employees are terminated or change positions, nor is this being detected through periodic access reviews.

Effect: Access to the EOSS departmental applications is not appropriately restricted which may result in inappropriate or unauthorized access or changes to EOSS data.

Recommendation: EOSS should establish and implement formalized access provisioning processes including periodic access reviews. In addition, a comprehensive access review of EOSS departmental applications should be performed, as our testing did not constitute a full access review. Generic accounts should be eliminated where possible.

Follow up should be performed with the appropriate application owners to ensure that appropriate visibility exists for terminated and transferred employees.

Management Response: Generic accounts were deactivated in two of the applications and all but a few in a third application the week of 4/29/2019.

Two of the applications have business and critical technical processes that depend on the remaining generic logins. The EOSS Technology Team will work with Housing and Career Professional and Development Services (CPDS) teams to define alternate processes and tools, if possible, so that generic logins can be removed without affecting service to students:

- Housing, by 6/30/2019
- CPDS, by 6/30/2019

Access control policies are already implemented in parts of EOSS. The EOSS Technology team will leverage these and implement them throughout EOSS

- Define and implement a communication plan to ensure EOSS departments know the ASU Policies related to data security, by 5/30/2019
- Create, document, communicate and deliver a standardized process to remove access by 6/30/2019
    - Establish departmental distribution lists for onboarding and offboarding employees
    - Establish checklists for access removal
    - Leverage existing daily termination and transfer reports
- Establish and schedule formalized, comprehensive, regular access review of EOSS applications listed as Critical/High, which contain Sensitive or Highly Sensitive data, starting with review of applications recently audited, by 6/30/2019. Reviews will be minimally quarterly.
- Continue to ensure that all EOSS staff completes the annual information security training (was at 99.7%)

2. Password configuration for EOSS departmental applications does not comply with the defined Information Security Password Standard.

Condition: The existing configuration for local privileged accounts and applications not utilizing SSO do not meet the defined Password Standard. Specifically, five of seven applications assessed did not meet the defined requirements of which one is due to system limitations of the application.

Criteria: ASU's Password Standard requires the following items:

- 10 character minimum
- 180 day reset for non-privileged and 90 day reset for privileged and
- The use of 3 of the 4 following attributes (upper, lower, digits and special)

Cause: Overall, for the systems that do not have system limitations related to password complexity, exceptions were generally related to the continued use of local accounts or generic accounts, which have not been configured to meet the defined requirements.

Effect: Passwords do not meet the defined complexity requirements increasing the risk of potential compromised credentials resulting in unauthorized access.

Recommendation: EOSS should update the existing configuration to meet the defined standard for hosted applications that support it. In addition, as part of the ongoing security risk assessments, EOSS should continue to assess the risk associated with using third party applications that do not meet ASU defined security provisions to determine if the risk is appropriately mitigated or if other vendors should be considered.

Management Response: Generic accounts were deactivated in two of the applications and but a few in a third application the week of 4/29/2019.

Two applications have business and critical technical processes that depend on the remaining generic logins. The EOSS Technology Team will work with Housing and Career Professional and Development Services (CPDS) teams to define alternate processes and tools, if possible, so that generic logins can be removed without affecting service to students:

- Housing, by 6/30/2019
- CPDS, by 6/30/2019

One application was modified to increase its password complexity to align with ASU standards on 5/6/2019.

Another application will transition to single sign on this summer, by 8/30/2019. This will eliminate the current limitations of the password not being compliant. In the interim, the EOSS Technology team will work with the department, vendor, and UTO to create compensating controls.

The EOSS Technology team will roll out processes and procedures to ensure ASU password rules are implemented across the board:

- Define and implement a communication plan to ensure EOSS departments know the ASU Policies related to data security, by 5/30/2019
- Incorporate password complexity into its risk assessment of new third party applications
- Include password complexity as a check item in internal access reviews and internal security assessments, by 5/24/2019.

3. Departmental applications are not accurately represented in the Continuity of Operations plans.

Condition: The seven departmental applications included in this review mapped to fourteen different Continuity of Operations plans. Within the 14 plans, the applications were considered non-deferrable systems (a recovery plan is required to be in place) 18 times. This is due to four of the seven applications being utilized in multiple areas of EOSS. Of the 18 instances, only five had complete and accurate information to support necessary recovery efforts.

Criteria: Continuity planning includes the creation of a strategy to address both the threats and risks facing EOSS including prioritizing functions and critical operations that are essential for recovery to ensure minimal impact to the university's overall objectives and goals. As part of the Emergency Planning and Security requirements, plans must be reviewed, updated, and tested annually.

Cause: Application owners are not involved in the creation of the Continuity of Operation plans.

Effect: With the exception of one application, departmental applications lacked sufficient information, were incorrectly labeled as centralized instead of departmental or were blank resulting in a high risk of inability to achieve a timely restoration in the event of a disruption.

Recommendation: Application owners should be involved with the annual update and review of the Continuity of Operation plans to ensure adequate information is captured to support recovery needs.

Management Response: While each plan is owned and filled out by each unit, the EOSS Technology team will take a greater role in ensuring the technology portion of each Continuity of Operations plan is filled correctly.

The EOSS Technology Team will contact each department and work with the department and vendor to add the missing information to the plans and correct any errors in categorization, by 6/15/2019.

The EOSS Technology Team will also work with Risk Management and Continuity of Operation plan oversight group to establish training protocols and communication with EOSS units, to improve overall understanding and expected methodologies needed to meet requirements by 7/30/2019.

Distribution:

Arizona Board of Regents Audit Committee
Michael M. Crow, President
Morgan R. Olsen, Executive Vice President, Treasurer, and Chief Financial Officer
James Rund, Senior Vice President Educational Outreach/Student Services
Jennifer Hightower, Vice President Student Services
Antoinette Farmer-Thompson, Deputy Vice President
Dara Foias, Chief Technology Officer, Student Services
Stephen Quick, Manager Information Technology
Kamala Rangaraju, Project Manager Information Technology
Heather Stevens, Project Manager Information Technology
Internal Audit Review Board