Arizona State University
Office of University Audits
General Computer Controls Audit
University Library
02/22/2019

This page intentionally left blank

Summary: The General Computer Controls (University Library) 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. This audit is in support of ASU's mission of preserving the availability, confidentiality and integrity of its information resources.

Background: General computer 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 general computer 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 the Library. 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 and that the continuity plan has been reviewed and tested within the past year
- Identify opportunities for improvement

Scope: The scope of the audit focused on assessing general computer controls for 10 high or medium risk departmental applications managed by the Library. Applications chosen included applications that contained sensitive information such as patron data as well as critical applications required to fulfill Library business objectives.

Control activities performed by the University Technology Office were not considered in scope for this review and therefore were not assessed.

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 validation were performed:
    - Validating unique user id's are utilized through review of access listing.
    - Performing a high-level access review based on job title and department.
    - Ensuring privileged access is appropriately restricted and provides adequate segregation of duties across the various application environments.
    - Reviewing password configuration to ensure password complexity requirements have been met.
    - Confirming application requires use of Port 443 to validate that data is encrypted during transit through inspection of connections.
    - Confirming applications have been implemented with full-disk encryption or that an encryption conversion plan has been submitted and approved by the Information Security Office.

  - Reviewing backup schedule configuration to validate backups are occurring.
  - Validating applications have a supported and current version of anti-malware software installed.
  - Validating application changes follow the defined Enterprise System Change Management Policy through inquiry with process owner.
  - Confirming applications are updated with vendor provided patches in a timely manner based on the defined Patch Management Policy through inquiry with the process owner.
  - Confirming applications are scanned according to the defined ASU Network Vulnerability Standard including tracking remediation efforts through reviewing results in Risk Sense.
  - Confirming applications have been configured to monitor activity as required by the System Audit Requirement Standard through inquiry with process owner.
- Validating the continuity of operations plan (COOP) is current and complete and that testing has been performed within the last 12 months.
- Assessing oversight of third party compliance to the defined security provisions through inquiry with the process owner and review of SOC2 reports where available.

Conclusion: Overall, Information Technology general computer controls have not been consistently implemented for applications managed by the Library. While some controls have been fully or partially implemented in the areas of encryption, anti-malware, and application backups, multiple exceptions were noted in the other areas including access management, password management, security reviews and logging/monitoring. In addition, the Library has not implemented the change management, patch management and vulnerability management standards within their environment. This is compounded by the lack of segregation between development and production environments. It was also noted that the continuity of operations plan was incomplete and missing relevant application information in addition to not being tested although it was marked as complete and current in the enterprise Kuali tool.

In addition, appropriate oversight over third party hosted applications has not been implemented to ensure compliance with the defined security provisions.

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			
• Automated backups of the departmental applications are performed and retained.	Reasonable to Strong Controls in Place.	N/A	N/A
Safeguarding of Assets		N/A	N/A
• Logical access to the departmental applications is appropriately restricted.	Opportunity for Improvement	1	7
• Password requirements and complexity configuration meet the defined Information Security Policy.	Opportunity for Improvement	2	8
• Antivirus protection is implemented to meet the defined Anti Malware Standard.	Opportunity for Improvement	3	9
• Encryption is implemented to meet the defined Data Handling Standard for data at rest and in transit.	Opportunity for Improvement	4	9
• Vulnerability management is implemented including review, analysis and remediation as defined by the Web Application and Network Security Standards.	Opportunity for Improvement	5	10
• Logging and monitoring is implemented to meet the defined System Audit Requirements Standard.	Opportunity for Improvement	6	10
• Change Management is implement to meet the defined Enterprise System Change Management Policy.	Opportunity for Improvement	7	11
• Patch Management is implemented to meet the defined Patch Management Standard.	Opportunity for Improvement	8	12
• Internal security reviews are in place to ensure technology purchases comply with ASU's Security Review requirements.	Opportunity for Improvement	9	13
• Third party vendor management oversight is implemented to ensure compliance with defined Security provisions.	Opportunity for Improvement	10	13
• The Continuity of Operations Plan is current, accurately reflects the Libraries applications, key personnel have been trained and the plan has been tested.	Opportunity for Improvement	11	15
Compliance with Laws and Regulations	Not Applicable	N/A	N/A

We appreciate the assistance of the University Library staff during the audit.

Lisa Grace, Executive Director, University Audit and Advisory Services
David Jones, IT Auditor, 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, 1 of 10 applications had inappropriate elevated level access. In addition, inappropriate user access was noted in 4 of the 5 applications reviewed. Exception rates of inappropriate access ranged from 2% - 13%.

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

Effect: Access to the Library departmental applications is not appropriately restricted which may result in inappropriate or unauthorized access or changes to Library data. This is compounded by the lack of segregation between development and production environments.

In two instances, it was noted that the application was accessed after the termination date.

Recommendation: The Library should establish and implement formalized access provisioning processes including periodic access reviews.

Management Response: ASU Library agrees it can improve its efforts related to this finding and will implement the following controls to address:

1) By 02/01/2019: Ensure all Technology Services staff are receiving PeopleSoft Termination and Transfer reports.

2) By 03/01/2019: Automate parsing of PeopleSoft Termination and Transfer reports to provide an "at-a-glance" notification of library-specific employees.

3) By 08/01/2019: Complete a full, systemic review of all applications and access, and repeat annually thereafter.

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

Condition: The existing configuration for local privileged accounts and applications not utilizing Single Sign On (SSO) does not meet the defined Password Standard.

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: For internally managed applications, configuration has not been set through use of Group policy for windows server or Ansibile for Linux to enforce password compliance.

It was also noted the hosted applications that do not utilize SSO had system limitations that do not allow compliance to password complexity requirements.

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

Recommendation: The Library should update the existing configuration to meet the defined standard for internally managed applications. In addition, as part of the ongoing security risk assessments, the Library 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: ASU Library agrees it can improve its efforts related to this finding, and will implement the following controls to address:

1) By 05/01/2019: Create and have employee sign-off on a "Password Guideline" that gives guidance on how to meet ASU's Password Standard.

2) By 07/01/2019: Ensure all configurable systems have controls in place to meet complexity requirements, including use of SSO if possible.

3) By 08/01/2019: Document and request risk acceptance where appropriate of all applications that cannot meet this standard.

3. Anti-malware controls for internally hosted applications require improvement.

Condition: Testing found that 1 in 3 (33%) of the internally hosted applications did not have malware protection enabled in violation of ASU's Anti Malware Standard.

Criteria: All devices connected to ASU's network must have a supported and current version of anti-malware software installed.

Cause: The Library did not implement anti-malware protection based on the nature of the application; however, this is in violation of the Anti-Malware Standard.

Effect: Applications that do not have anti-malware installed have increased exposure to malware threats, increased risk of data privacy issues, and other potential security or performance issues.

Recommendation: The Library should implement an anti-malware solution compliant with ASU's Anti-Malware Standard.

Management Response: ASU Library agrees it can improve its efforts related to this finding, and will implement the following controls to address:

1) By 05/01/2019: Ensure all systems have ASU's new "CrowdStrike" anti-malware solution installed.

4. Encryption controls for Library departmental applications do not comply with ASU's Data Handling Standard.

Condition: The Library has data classified as sensitive that is not encrypted at rest in violation of ASU's Data Handling Standard.

Criteria: ASU's Data Handling Standard requires that data classified as sensitive be encrypted at rest.

Cause: The Library identified data that was classified as sensitive; however, did not take necessary steps to move data to a secured storage location utilizing full-disk encryption nor has an encryption conversion plan been filed with the Information Security office.

Effect: Sensitive and highly sensitive data is not encrypted at rest resulting in increased risk of unauthorized access.

Recommendation: The Library should submit an encryption conversion plan with the Information Security office resulting in full disk encryption of sensitive data at rest.

Management Response: ASU Library agrees it can improve its efforts related to this finding, and will implement the following controls to address:

1) By 08/01/2019: Migrate the ILLiad service to Amazon Web Services (AWS) to take advantage of “at rest” encryption controls that would be too costly to implement internally.

5. The Library has not implemented the ASU Network Vulnerability Management Standard for departmentally managed applications.

Condition: Vulnerability Management has not been formally implemented in violation of ASU’s Network Vulnerability Management Standard.

Criteria: The Vulnerability Management Standard requires that all ASU technology zones be scanned for the identification, classification, remediation and mitigation of vulnerabilities in a timely manner.

Cause: Applications are not scanned and formally tracked within Risk Sense.

Effect: Vulnerabilities are not identified, assessed, nor remediated resulting in increased risk of exposure of application confidentiality, availability and integrity.

Recommendation: The Library should implement the Network Vulnerability Management Standard for departmentally managed systems.

Management Response: ASU Library agrees it can improve its efforts related to this finding, and will implement the following controls to address:

1) By 03/01/2019: Ensure proper configuration of library networks in RiskSense.

2) By 04/01/2019: Complete systemic review of all library web applications, owners, and configuration for RiskSense scanning.

3) By 08/01/2019: Updated configuration compliant with vulnerability management standards.

6. The Library has not consistently implemented logging and monitoring controls for departmentally managed applications.

Condition: Logging and monitoring is not consistently implemented for the departmentally managed applications. Specifically, logging and monitoring is not in place

for 2 of 3 (66%) applications reviewed. In both instances, the applications are categorized as highly sensitive or sensitive which is in violation of ASU's Server Security Standard.

Criteria: All systems that require high availability and handle sensitive or highly sensitive information must record and retain audit-logging information sufficient to answer what activity was performed, who performed the activity, what object the activity was performed on, when the activity was performed, what tools were utilized and what the impact was.

Cause: The Library has not consistently implemented logging and monitoring across their environment.

Effect: Logging and monitoring of internally managed applications are not adequate which may result in failure to detect inappropriate access or changes to Library data.

Recommendation: The Library should extend the logging and monitoring controls to include all internally managed applications in compliance with the ASU Server Security Standard.

Management Response: ASU Library agrees it can improve its efforts related to this finding, and will implement the following controls to address:

1) By 05/01/2019: Ensure all internally hosted applications have logs sent to Splunk.

2) By 08/01/2019: Ensure all internally hosted applications have appropriate monitoring in place in Splunk.

7. The Library has not implemented the Enterprise System Change Management Standard for departmentally managed applications.

Condition: Change management has not be formally implemented in violation of ASU's Server Security Standard.

Criteria: ASU's Enterprise System Change Management Standard establishes a requirement for a formal change management process. It provides a framework for evaluating, reviewing, approving, scheduling, communicating, implementing and documenting changes to ASU's technology systems.

Cause: Changes are managed internally and informally resulting in no formal documentation.

Effect: Changes made to Library resources do not follow the defined framework ensuring that all changes have been assessed in a thoughtful manner that minimizes impact to

services. This is compounded by the lack of segregation between development and production environments.

Recommendation: The Library should implement the Enterprise System Change Management Standard for departmentally managed systems.

Management Response: ASU Library agrees it can improve its efforts related to this finding, and will implement the following controls to address:

1) By 02/01/2019: Establish a Slack channel to communicate changes to production systems.

2) By 08/01/2019: Establish risk-based, documented change management procedures for its technologies at an agreed upon level by application owners and library leadership.

8. The Library has not implemented the ASU Patch Management Standard for departmentally managed applications.

Condition: Patch management has not been formally implemented in violation of ASU's Server Security Standard.

Criteria: The Patch Management Standard requires that patches be applied to all software, including OS and individual application patches, immediately, or as soon as possible, following an appropriate testing cycle of the security patches by the individual or team responsible for the device or system.

Cause: Patch management is not formally tracked or documented.

Effect: Patches are not assessed and applied in a timely manner resulting in increased risk of exposure of application data integrity and availability.

Recommendation: The Library should implement the ASU Patch Management Standard for departmentally managed systems.

Management Response: ASU Library agrees it can improve its efforts related to this finding, and will implement the following controls to address:

1) By 03/01/2019: Ensure all patching is communicated in the newly created change management channel in Slack, which will serve as a formal record.

9. Internal security reviews for technology purchases are not being performed or are not documented.

Condition: Internal security reviews for technology purchases are not formalized or documented in violation of ASU's Security Review requirements.

Criteria: ASU requires that departments purchasing and implementing software and technology also implement appropriate security controls to safeguard university assets. Specifically, for software or technology that is not new to the university and does not have new integrations to ASU's network, the technical lead for the department is required to complete an internal security review.

Cause: The Library has not implemented processes to ensure that required security reviews are performed and documented.

Effect: For three of the applications assessed that were renewed during our review period (covered by the same invoice), the required internal security review was not performed although it was marked as complete by the purchaser.

Recommendation: The Library should formalize their internal security review process to ensure all software purchases follow the defined process including reassessing applications at time of renewal to ensure current use, and integrations have not changed.

Management Response: ASU Library agrees it can improve its efforts related to this finding and will implement the following controls to address:

1) By 8/01/2019: Ensure all medium / high criticality applications have reviews documented in Service Now, and that a business process is in place to ensure other technologies have a documented security review when purchased or renewed.

10. The Library has not implemented appropriate vendor management processes over third parties to ensure compliance with required security provisions.

Condition: The Library has not implemented adequate third party oversight monitoring processes of vendors to ensure they are compliant with the required security provisions of the contract.

Criteria: As part of standard contract language, ASU requires that all systems containing ASU data must be designed, managed, and operated in accordance with information security best practices. The entity must meet specific requirements around access control, incident reporting, patch management, encryption, security reviews, scanning

and penetration tests, and secure development. It is the application owner's responsibility to monitor and ensure compliance with these provisions.

Cause: The Library has not implemented oversight processes to ensure third party compliance with security provisions.

Effect: Seven of the applications reviewed involved the use of third parties. The vast majority of the third party providers do not provide SOC 2 reviews for their application and in the few instances where they did; the Library was not requesting or reviewing. For those that do not offer a SOC 2, processes have not been implemented to assess compliance with security provisions. As such, it is unknown if those applications are compliant or not. Types of ASU data maintained in the applications managed by third party service providers include high criticality and high availability services such as its websites and sensitive patron data.

Recommendation: The Library should implement formal procedures to monitor third party compliance with required security provisions. This should include annual certification where the third party does not provide SOC2 reviews of their application and environment.

Management Response: ASU Library agrees it can improve its efforts related to this finding and will implement the following controls to address:

1) By 04/01/2019: Complete systemic review of applications and their criticality, availability, and data sensitivity ratings.

2) By 05/01/2019: Verify contract status of third-party applications with business manager

3) By 08/01/2019: Document compliance status of third-party applications in Service Now or other appropriate location.

11. The Continuity of Operations Plan is not complete and has not been tested.

Condition: The existing Continuity of Operations (COOP) plan for the Library was marked complete and up-to-date in the Kuali tool; however, it does not represent the current applications utilized by the Library and has not been tested.

Criteria: Continuity planning includes the creation of a strategy to address both the threats and risks facing the Library 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: There was an enterprise wide deadline to review, update and test Continuity of Operation Plans by October 31, 2018. Although this had not been completed, the Library reported the plan was complete in order to meet the defined deadline.

Effect: The existing plan does not contain all applications that have been identified as high or medium risk and therefore has not established nor tested recovery strategies to ensure these applications can be recovered to support defined goals and objectives of the Library.

Recommendation: The University Library should complete the Continuity of Operations Plan, which includes developing necessary recovery strategies and prioritization of the critical functions and operations across the Library. In addition, the plan should be tested to identify potential gaps and to facilitate overall awareness and training of the plan.

Management Response: ASU Library agrees it can improve its efforts related to this finding, and will implement the following controls to address:

1) By 08/01/2019: Ensure the Continuity of Operations Plan is up-to-date and that its components have been tested.

Distribution:

Arizona Board of Regents Audit Committee
Michael M. Crow, President
Morgan R. Olsen, Executive Vice President, Treasurer and Chief Financial Officer
Mark Searle, Executive Vice President, University Provost
Sheila Ainlay, Vice Provost
James O'Donnell, University Librarian & Professor
Debra Hanken Kurtz, Associate University Librarian
Jeremy Kurtz, Director System Infrastructure & Security
Internal Audit Review Board