Arizona State University
Office of University Audits
Information Technology General Controls
W. P. Carey School of Business
November 23, 2020

Summary: The Information Technology General Controls audit was included in the Arizona State University (ASU) FY 2020 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 applications managed by W. P. Carey Technology Services. 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:

<u>Access Management:</u> 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

<u>Change Management:</u> 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

<u>Computer Operations:</u> 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
- Server Security 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.

Audit Objective: The objective of this engagement was to assess the design and effectiveness of general computer controls managed within W. P. Carey School of Business. 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, malware and firewall protection.
- 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 five medium-risk departmental applications managed by to W. P. Carey School of Business Technology Services. Applications chosen included applications that contained student data including advising, leads, application and admissions tasks as well as classroom access controls.

Control activities performed by the University Technology Office were not considered in scope for this review and therefore were not assessed. As such, backups, antivirus and firewall protection, logging/monitoring, and encryption at rest were not assessed for UTO hosted or managed applications.

W. P. Carey departmental applications are part of the university managed vulnerability management environment and are being scanned based on ASU's defined guidelines; however no high or critical vulnerabilities were identified for the in-scope applications during the audit timeframe. As a result, timeliness of vulnerability remediation could not be assessed. In addition, W. P. Carey recently transitioned to JIRA for change management tracking. There was not an adequate population of changes to conclude as part of this review. Procedures were performed on the available changes and feedback provided to the unit where documentation did not align with the Enterprise Change Management Standard.

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:

- Validating Logical Access through the following procedures:

  - 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 FERPA training requirements were met.
  - Ensuring privileged access is appropriately restricted.
  - Ensuring access is restricted to affiliated individuals.
- Reviewing password configuration to ensure password complexity requirements have been met.
- Reviewing backup schedule configuration to confirm backups are occurring.
- Confirming applications have been implemented with full-desk encryption to validate that data is encrypted at rest through inquiry with the process owner.
- Confirming applications require use of Port 443 to validate that data is encrypted during transit through inspection of connections.
- Confirming applications are updated with vendor provided patches in a timely manner based on the defined Patch Management Standard.
- Confirming applications have been implemented with malware protection as required by the Antimalware Standard through inspection of configurations.
- Confirming applications have been implement with firewall protections as required by the Antimalware Standard through inspection of configurations.
- Confirming applications have been configured to monitor activity as required by the System Audit Requirement Standard.
- Validating that the continuity of operation plan accurately represent the departmental applications.

Conclusion: Overall, W. P. Carey School of Business has implemented effective information technology controls related to password requirements/complexity, encryption in transit, malware and firewall protection, patch management and continuity of operations planning; however, further improvement is needed to ensure controls are operating as intended in the areas of logical access, logging and monitoring and encryption at rest.

Testing indicated that logical access was not appropriately restricted in three of the five applications reviewed with exception rates ranging from 17%-19% for non-privileged accounts. Formalized access reviews were not in place, which would have detected the inappropriate access. In addition, privileged access was not provisioned through exception accounts as required by the Privileged Account Standard. It was also noted that 4 of 5 applications have data not encrypted at rest as required by the Data Handling 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			
• Automated backups of the departmental applications are performed and retained.	Reasonable to Strong Controls in Place	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.	Reasonable to Strong Controls in Place	N/A	N/A
• Antivirus protection is implemented to meet the defined Antimalware Standard	Reasonable to Strong Controls in Place	N/A	N/A
• Firewall protection is implemented to meet the defined Antimalware Standard	Reasonable to Strong Controls in Place	N/A	N/A
• Encryption is implemented to meet the defined Data Handling Standard for data in transit and at rest.	Opportunity for Improvement	2	7
• Logging and monitoring is implemented to meet the defined System Audit Requirements Standard.	Opportunity for Improvement	3	8
• Patch Management is implemented to meet the defined Patch Management Standard.	Reasonable to Strong Controls in Place	N/A	N/A
• Departmental applications are accurately reflected in the continuity of operations Plan.	Reasonable to Strong Controls in Place	N/A	N/A
Compliance with Laws and Regulations	Not Applicable		

We appreciate the assistance of the W. P. Carey staff during the audit.

Lisa Grace, Executive Director, University Audit and Advisory Services
David Jones, Senior 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, inappropriate user access was noted in three of five applications reviewed with exception rates ranging from 17%-19% for non-privileged access.

It was also noted that privileged access for all applications was provisioned to ASURite credentials in violation of ASU's Privileged Account Standard, which requires the use of exception accounts.

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. In addition, ASU's Privileged Accounts Standard requires privileged access to be provisioned to an exception account to ensure least privilege.

Cause: Application owners are responsible for granting/removing access to departmental applications; however, formalized provisioning processes are not in place for all applications. Testing indicated that for three of the applications, the system administrators are dependent on departments notifying them when access should be removed which is not occurring consistently. Formal access reviews have not been implemented which would have detected the inappropriate access.

Effect: Access to departmental applications is not appropriately restricted, which may result in inappropriate or unauthorized access or changes to data. Types of data include applications that contained student data including advising, leads, application and admissions tasks as well as classroom reservation and access controls.

Recommendation: Full access reviews should be performed on all applications to ensure access is appropriate. Testing did not constitute a full access review so additional incidents of inappropriate access may exist given the lack of formalized processes. Technology Services should also formalize access-provisioning processes to ensure access is removed when no longer required. Periodic access reviews should also be implemented across all applications to ensure access is appropriately restricted.

In addition, privileged access should be migrated to exception accounts as required by the Privileged Account Standard where applicable.

Management Response: Beginning January 2021, Technology services will perform full access reviews quarterly on all departmental applications. In addition, beginning December 2020, the current provisioning process using ServiceNow tickets initiated by WPC Human Resources will continue and be combined with a review of a bi-weekly report provided by Human Resources to identify hires, job changes and terminations.

Privileged access will be migrated to exception accounts where possible in January 2021.

2. Encryption controls for W. P. Carey School of Business departmental applications do not comply with ASU's Data Handling Standard.

Condition: W. P. Carey School of Business 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: W. P. Carey Technology Services identified data that was classified as sensitive; however, the data resides on servers that do not support encryption requirements. Necessary steps to move data to a secured storage location utilizing full-disk encryption has not been done nor has an encryption conversion plan been filed with the Information Security office.

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

Recommendation: W. P. Carey Technology Services should submit an encryption conversion plan with the Information Security office documenting their plan of bringing applications compliant with encryption requirements.

Management Response: Technology Services is currently working with UTO to migrate the servers which cannot be encrypted at rest due to hardware and software limitations to a combined infrastructure of cloud and on-premise servers which will be configured to encrypt at rest. This project is expected to be complete by April, 2021.

3. Logging and monitoring controls do not comply with the System Audit Requirement Standard.

Condition: All applications had logging enabled; however, logs are not retained for a minimum of one year as required by the System Audit Requirement Standard.

Criteria: ASU's System Audit Requirement Standard requires that severs log event data sufficient to answer the activity performed, who or what performed the activity including what system the activity was performed from, when the activity was performed, what tools were utilized and the status or result of the activity. Logs must be retained for no less than 1 year and be periodically reviewed.

Cause: Group policy enforcing audit logging was present on the servers; however, it is configured to 510mb before overwriting previous data. The servers are end of life and when the virtual machines were created, the configuration was set at 510mb.

Effect: Servers have the capacity to retain 5-8 months of log history depending on the server.

Recommendation: Management should formalize their plan to address the end of life servers, factoring in retention requirements. If replacement will not be done in a timely manner, risk acceptance should be obtained from the accountable administrator.

Management Response: Technology Services is currently working with UTO to migrate the servers with the limitations noted above to a combined infrastructure of cloud and on-premise servers. The replacement servers will be configured to retain 12 months of log event data. This project is expected to be complete by April, 2021.

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 & Professor
Amy Hillman, Dean & Professor, W. P. Carey School of Business
Sheila Ainlay, Vice Provost
Anne Nguyen, Assistant Dean – Services, W .P. Carey School of Business
Robin Gonzalez, Director of Technology Projects and Operations, W.P. Carey School of Business
Tracy Howell, Manager, W. P. Carey School of Business
Internal Audit Review Board

This page intentionally left blank.