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 undergraduate admission applications managed by Enrollment 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:

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 Enrollment Services. 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 five high or medium-risk departmental applications managed by Enrollment Services related to undergraduate admissions. Applications chosen included applications that contained student, scholarship, recruitment data as well as an application that supports a critical Admissions Services business function.

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 protection and encryption at rest were not assessed for UTO hosted applications.

Enrollment Services departmental applications are part of the university managed vulnerability management RiskSense environment and they are scanned by ASU's defined guidelines, however no high or critical vulnerabilities were identified for the in-scope applications during the audit timeframe so testing of vulnerability remediation timeliness was not performed as part of this 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:

- 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.
- Confirming applications require use of Port 443 to validate that data is encrypted during transit through inspection of connections.
- Validating application changes follow the defined Enterprise System Change Management Standard.
- Confirming applications are updated with vendor provided patches in a timely manner based on the defined Patch Management Standard.
- Confirming applications are scanned according to the defined Vulnerability Management Security 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.
- 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 operation plan accurately represent the departmental applications.

**Conclusion:** Overall, Enrollment Services has implemented effective information technology controls related to change/patch management, encryption in transit, vulnerability management, logging and monitoring; however, further improvement is needed to ensure controls are operating as intended in the areas of logical access, password requirements/complexity and vendor oversight. It was also noted that the continuity of operation plan lacked accurate application data to ensure recovery.

Specifically, testing indicated that logical access was not appropriately restricted in four of the five applications reviewed with exception rates ranging from 20%-38% for privileged access and 9%-49% for non-privileged. 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. Testing also identified one instance where password configuration had not been configured adequately for a hosted application. This was remediated during the review; however, it is recommended that a full review of third party applications is performed to ensure all systems are configured to meet the defined password standard.
It was also noted that Enrollment Services has implemented some processes to manage third party service provider oversight including collecting SOC2 reports and vulnerability scans from third parties where relevant; however, formal assessment processes have not been consistently implemented to ensure collected information is reviewed to verify ASU data is adequately secured.

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

<table>
<thead>
<tr>
<th>General Control Standard</th>
<th>Control Environment</th>
<th>Finding No.</th>
<th>Page No.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reliability and Integrity of Financial and Operational Information</td>
<td>Not Applicable</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>Effectiveness and Efficiency of Operations</td>
<td>Not Applicable</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>Safeguarding of Assets</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Logical access to the departmental applications is appropriately restricted.</td>
<td>Opportunity for Improvement</td>
<td>1</td>
<td>7</td>
</tr>
<tr>
<td>• Password requirements and complexity configuration meet the defined Information Security Policy.</td>
<td>Opportunity for Improvement</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>• Encryption is implemented to meet the defined Data Handling Standard for data in transit.</td>
<td>Reasonable to Strong Controls in Place</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>• Vulnerability management is implemented including review, analysis, and remediation as defined by the Web Application and Network Security Standards.</td>
<td>Reasonable to Strong Controls in Place</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>• Logging and monitoring is implemented to meet the defined System Audit Requirements Standard.</td>
<td>Reasonable to Strong Controls in Place</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>• Change Management is implemented to meet the defined Enterprise System Change Management Policy.</td>
<td>Reasonable to Strong Controls in Place</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>• Patch Management is implemented to meet the defined Patch Management Standard.</td>
<td>Reasonable to Strong Controls in Place</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>• Internal security reviews are in place to ensure technology purchases comply with ASU’s Security Review requirements.</td>
<td>Reasonable to Strong Controls in Place</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>• Third party vendor management oversight is implemented to ensure compliance with defined</td>
<td>Opportunity for Improvement</td>
<td>2</td>
<td>8</td>
</tr>
</tbody>
</table>
Security provisions.

- Departmental applications are accurately reflected in the continuity of operations Plan.

<table>
<thead>
<tr>
<th>Compliance with Laws and Regulations</th>
<th>Not Applicable</th>
</tr>
</thead>
</table>

Opportunity for Improvement 3 9

We appreciate the assistance of the Enrollment Services staff during the audit.

Lisa Grace, Executive Director, University Audit and Advisory Services
David Jones, SR 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 four of five applications reviewed with exception rates ranging from 20%-38% for privileged and 9%-49% for non-privileged access.

In addition, the following items were noted as part of testing:

- Two applications had inappropriate privileged level access.
- Four applications had inappropriate non-privileged level access.
- 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 four 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.

In one instance, it was noted that Enrollment Services provisions administrator level access for other departments who then further provision privileged and non-privileged access for their department of which those departments are also not actively managing 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 student data, recruitment data, predictive analytics, and scholarship data. One of the four applications is identified as a tier one critical system for the university.

**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.
Enrollment 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:** Enrollment Services application owners will perform a full access review of all their respective applications. A formalized provisioning process will be implemented including periodic access reviews. This process will be implemented by 6/1/2020.

Enrollment Services is working with the University Technology Office’s GPIS team to get clarification of how ASU’s Privileged Account Standard applies to the applications in question. Enrollment Services will then update applications to comply with the standard.

2. Enrollment Services has not fully implemented adequate vendor management processes over third parties to ensure compliance with required security provisions.

**Condition:** Enrollment Services has implemented some processes to manage third party service provider oversight including collecting SOC2 reports and vulnerability scans from third parties where relevant; however, formal assessment processes have not been implemented to ensure collected information is reviewed to verify ASU data is adequately secured.

**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:** Enrollment Services has implemented processes to assess third party applications through the security review process, in addition they have implemented processes to collect the SOC2 reports and vulnerability scans annually as relevant; however, formal assessment controls were not being performed consistently.

**Effect:** Third party applications have not been assessed to ensure ASU data is properly secured and follow the required information security contractual provisions.
**Recommendation:** Enrollment Services should implement additional oversight of application administrators to ensure the required vendor oversight activities are performed annually.

**Management Response:** Enrollment Services will implement a formal process to annually assess SOC2 reports and vulnerability scans for third party applications by 4/1/2020.

### 3. The Enrollment Services continuity of operation plan is not complete as it relates to departmental applications.

**Condition:** Departmental applications are not included in the continuity of operations plan or in some cases, are included but do not have the necessary detail to support recovery efforts.

**Criteria:** Continuity planning includes the creation of a strategy to address both the threats and risks facing Enrollment Services 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:** Enrollment Services has not consistently involved application owners in the creation and updating of the continuity of operation plan.

**Effect:** Two of the three applications reviewed were not captured in the continuity plan or did not include required information to support recovery efforts.

Review of the Enrollment Services Plan indicated that multiple applications included do not contain the necessary data to support recovery efforts resulting in a high risk of not achieving 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 plan to ensure adequate information is maintained to support recovery needs. While the two applications noted as exceptions as part of this review were updated during the course of the audit, a full review of all applications is necessary to ensure plans contain appropriate level of detail.

**Management Response:** Enrollment Services Sr. TAG representative will perform a full review of the continuity of operations plan with application owners to ensure that it includes adequate detail to support recovery by 5/1/2020. The plan will then be updated.
as new applications are added to the Enrollment Services inventory and reviewed annually with the application owners.
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
Kent Hopkins, Vice President Enrollment Management and Services
Sheila Ainlay, Vice Provost
Matthew Lopez, Associate Vice President, Enrollment Services
Chris Geary, Senior Director Information Systems Development
Internal Audit Review Board
This page intentionally left blank