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 Knowledge Enterprise Development. 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
- Privileged Accounts Standard
- Access to University Technology Resources and Services Policy
- 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
- Web Application Security Standard
- Patch Management Standard
- Anti-Malware Standard
- Systems Audit Requirements 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 Knowledge Enterprise Development. 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 six high or medium-risk departmental applications managed by Knowledge Enterprise Development. Applications chosen included applications that contained lab inventory and locations, billing and chargeback data, key information related to research and sponsored projects, as well as Knowledge Enterprise Development operational data.

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:

- 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 training requirements were met.
  - Ensuring privileged access is appropriately restricted.
  - Ensuring access is restricted to affiliated individuals.
- 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 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.

Reviewing backup schedule configuration to confirm backups are occurring.

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 operations plans (COOPs) accurately represent the departmental applications.

**Conclusion:** Overall, Knowledge Enterprise Development has implemented effective information technology controls related to change/patch management, encryption in transit, logging and monitoring, backups, and password complexity; however, further improvement is needed to ensure controls are operating as intended in the areas of logical access, vulnerability management, and vendor oversight.

Specifically, testing indicated that logical access was not appropriately restricted in four of the six applications reviewed with exception rates ranging from 4%-25% for privileged access and 5%-13% 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.

In addition, Knowledge Enterprise Development has not implemented processes to manage third party service provider oversight. As a result, neither SOC2 reports nor the required vulnerability scans had been collected and assessed for either of the hosted applications reviewed.
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></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Automated backups of the departmental applications are performed and retained.</td>
<td>Reasonable to Strong Controls in Place</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>Reasonable to Strong Controls in Place</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>• Antivirus protection is implemented to meet the defined Anti Malware Standard.</td>
<td>Reasonable to Strong Controls in Place</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>• Encryption is implemented to meet the defined Data Handling Standard for data at rest and in transit.</td>
<td>Opportunity for Improvement</td>
<td>2</td>
<td>8</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>Opportunity for Improvement</td>
<td>3</td>
<td>9</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 Security provisions.</td>
<td>Opportunity for Improvement</td>
<td>4</td>
<td>10</td>
</tr>
</tbody>
</table>
- Departmental applications are accurately reflected in the Continuity of Operations Plans.

<table>
<thead>
<tr>
<th>Compliance with Laws and Regulations</th>
<th>Reasonable to Strong Controls in Place</th>
<th>N/A</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Not Applicable</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

We appreciate the assistance of the Knowledge Enterprise Development 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 the six applications reviewed with exception rates ranging from 3%-25% for privileged and 5%-13% for non-privileged access.

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

- Three applications had inappropriate administrator level access.
- One application had privileged (Principle Investigator) access provisioned to non-affiliated users, which was intentional by design; however, access has not been proactively managed resulting in external access not being removed as required.
- 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 two of the applications, the system administrators are dependent on departments notifying them when access should be removed which is not occurring consistently. For one application, which is hosted through a 3rd party, deprovisioning processes had not been implemented at all.

The remaining application had inappropriate local administrator access provisioned to individuals that are not ASU affiliates. This access was no longer required due to the application moving to single sign on; however, local accounts were not removed. This access was removed during the audit.

Effect: Access to the Knowledge Enterprise Development departmental applications is not appropriately restricted, which may result in inappropriate or unauthorized access or changes to data. Types of data include lab inventory and locations, billing and chargeback data, as well as Knowledge Enterprise Development operational data.
**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.

Knowledge Enterprise Development should 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.

**Management Response:** To address privileged access, KE will implement exception accounts for all staff performing administrative work on the identified systems. System administrators will be systematically prompted to perform formalized access reviews on all applications noted.

To address non-privileged access in systems where this issue was noted, KE is working toward access removal by connecting via LDAP to verify and remove accounts which have been terminated. This has been deemed low-risk as data available to terminated employees within these systems is limited to their own research information.

2. **Encryption controls for Knowledge Enterprise Development departmental applications do not comply with ASU’s Data Handling Standard.**

**Condition:** Four of the six applications tested were not encrypted at rest in violation of ASU’s Secure Web Development Standard.

**Criteria:** ASU’s Secure Web Development standard requires that medium or high-risk applications utilize full-disk encryption to encrypt data at rest.

**Cause:** Knowledge Enterprise Development has not implemented full-disk encryption nor has an encryption conversion plan been filed with the Information Security Office for the four applications. For three of the applications, the current hosted environment does not support encryption at rest.

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

**Recommendation:** Knowledge Enterprise Development should implement full-disk encryption for the one application where functionality is supported. For the remaining three applications where functionality is not supported, Knowledge Enterprise
Development should work with Information Security Office to develop a plan to address compliance.

**Management Response:** On December 18th, the SCSM instance was moved to a server within Research Computing that has full disk encryption. For additional systems identified where encryption-at-rest is not supported, KE is actively considering pathways to compliance and whether data involved warrants this level of added protection/cost.

3. **Knowledge Enterprise Development has not implemented the ASU Network Vulnerability Management Standard for all departmentally managed applications.**

**Condition:** Vulnerability Management has not been formally implemented in one of the four applications 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:** Overall, Knowledge Enterprise Development generally follows the Vulnerability Management Standard for departmentally managed applications. For the one exception noted, the system administrator thought the application was included in the scans; however, it was not in error.

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

**Recommendation:** In addition to including the application noted in tested in the recurring scan activity, Knowledge Enterprise Development should perform a full review of their applications to ensure all applications are being scanned as intended.

**Management Response:** All IP addresses for SCSM have been added to RiskSense for vulnerability scanning.
4. **Knowledge Enterprise Development has not implemented appropriate vendor management processes over third parties to ensure compliance with required security provisions.**

**Condition:** Knowledge Enterprise Development 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:** Currently, the application owner is responsible for ongoing vendor management activities; however, these individuals were not aware of the annual requirements related to third party service providers.

**Effect:** Knowledge Enterprise Development has not implemented processes to manage third party service provider oversight. As a result, neither SOC2 reports nor the required vulnerability scans had been collected and assessed for either of the hosted applications reviewed as required by the Web Application Security Standard.

**Recommendation:** Research Technology Office Information Security should implement additional oversight of application administrators to ensure the required vendor oversight activities are performed annually.

**Management Response:** Knowledge Enterprise is piloting, with support from the campus information security office, use of the Higher Education Community Vendor Assessment Tool (HECVAT) to satisfy this review requirement for identified applications.
Distribution:

Arizona Board of Regents Audit Committee
Michael M. Crow, President
Morgan R. Olsen, Executive Vice President, Treasurer, and Chief Financial Officer
Sethuraman Panchanathan, Executive Vice President, Chief Research and Innovation Officer
Tamara Deuser, Associate Vice President and Chief Operations Officer
Sean Dudley, Assistant Vice President and Chief Information Officer
Zachary Jetson, Information Security Specialist Senior
Internal Audit Review Board