This page intentionally left blank
Summary: The Configuration Management 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 departmental servers that are managed through the University Technology Office (UTO). This audit is in support of ASU’s mission of preserving the availability, confidentiality, and integrity of its information resources.

Background: Configuration Management is the process of implementing and maintaining standard settings and changes to network hardware and software over the life cycle of the system to ensure it performs as intended and is documented in sufficient detail. Many of these configuration settings have a direct impact on the overall security of that system.

ASU has implemented the Server Security Standard to define the base configuration requirements of server equipment. The standard addresses areas of logical access, password configuration, physical access, operating system configuration settings, logging, patching, backups, and other security focused areas to protect and maintain a secure environment.

The UTO manages all enterprise servers as well as many departmental servers. In addition, individual college or business units may also manage departmental servers.

Audit Objective: The objective of this engagement was to assess the design and effectiveness of controls in place for departmental servers that are hosted by the UTO including the following areas:

- Ensure logical access is appropriately restricted and follows the Privileged Account Standard
- Ensure multifactor authentication is implemented and that privileged access is performed over secure methods
- Ensure the passwords comply with the Password Standard and that default passwords are changed
- Ensure servers have defined backup schedules
- Ensure security patches are installed in accordance with the Patch Management Standard
- Ensure appropriate logging is implemented in accordance with the System Audit Requirement Standard
- Ensure server changes comply with the Enterprise Change Management Standard
- Ensure data on servers is encrypted at rest
- Ensure servers follow the established standardized image for standard secure configurations
Scope: The scope of the audit focused on 42 departmental servers that are managed through the UTO representing key applications previously covered as part of departmental Information Technology General Control Application audits. The application audits focused on departmental owned controls where this audit is addressing the server controls managed through the UTO.

Vulnerability Management processes were initially included the scope of this review; however, it was confirmed that the population of critical and high vulnerabilities related to the selected servers was not adequate to base testing on. As a result, vulnerability management was not tested as part of this review and will be addressed as part of the planned FY2021 audit focused on enterprise level vulnerability management.

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 various University Technology teams, observation of work processes, review of documented policies and procedures and substantive tests including the following areas:

- Ensuring standard images of operating system have been developed through review of the installation and configuration checklist
- For a sample of 42 departmental servers, performed the following:
  - 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
    - 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 default passwords have been changed through inspection of configuration settings if applicable, otherwise through inquiry with local account owner
  - Confirming server data is encrypted at rest through inspection of configuration settings
  - For a sample of 112 changes (including patches), across the 42 servers, validating server changes followed the defined Enterprise System Change Management Standard
  - Validating servers have been configured to monitor activity as required by the System Audit Requirement Standard through inspection of configuration
settings and confirming logging detail through the enterprise SPLUNK application
  o Validating servers have been configured with a malware solution that complies with the Antimalware Standard through inspection of configuration settings
  o Validating server backups are configured to comply with the Server Security Standard through obtaining system configuration of back up schedules
  o Validating servers have firewalls configured to comply with the Server Security Standard through inspection of configuration

Conclusion: Overall, the University Technology Office has generally implemented effective controls to ensure servers comply with the base configuration requirements defined by the Server Security Standard, although additional improvement is needed in the areas of privileged exception accounts, logging activities and change management processes.

Testing identified that exception accounts are not consistently utilized to provision privileged account. Specifically, of the servers reviewed, 40% (38 of 95) of the accounts were standard accounts rather than an exception account as required. Provisioning privileged access to a standard account increases the overall risk of compromised credentials across the university’s network.

In addition, it was noted that while controls had been implemented to capture necessary logging activity, there was a group policy conflict which resulted in 14 of the 42 (33%) servers not capturing logging as intended. Change management processes have also been implemented and generally follow the enterprise change management policy; however, require further improvement. Specifically, the planning aspect of the change record is not consistently documented, which is important to ensure there is consideration of necessary steps if the change does not go as planned. Testing identified that 36% of the changes reviewed (40 of 112) did not have the planning components of the change documented.

It was also noted that servers are generally configured with appropriate encryption and malware protection; however, in some instances system limitations prevented these controls from being implemented due to servers being end of life or unsupported. While these servers are part of the current migration plan to AWS, it is important to note that some of these servers are running applications that are mission critical to ASU.
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>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>Effectiveness and Efficiency of Operations</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>• Automated backups of the departmental servers 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 departmental servers is appropriately restricted.</td>
<td>Reasonable to Strong Controls in Place</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>• Privileged accounts meet the defined Privileged Account Standard.</td>
<td>Opportunity for Improvement</td>
<td>1</td>
<td>6</td>
</tr>
<tr>
<td>• Multifactor authentication is implemented and privileged access is performed over secure methods.</td>
<td>Reasonable to Strong Controls in Place</td>
<td>N/A</td>
<td>N/A</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>• Default passwords are changed at implementation as defined by the Server Security Standard.</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 Server Security Standard for data at rest.</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>Opportunity for Improvement</td>
<td>2</td>
<td>7</td>
</tr>
<tr>
<td>• Change Management is implemented to meet the defined Enterprise System Change Management Policy.</td>
<td>Opportunity for Improvement</td>
<td>3</td>
<td>7</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>
</tbody>
</table>
Firewalls are implemented to meet the defined Server Security Standard.

| Reasonable to Strong Controls in Place | N/A | N/A |

We appreciate the assistance of the University Technology Office during the audit.

Lisa Grace, Executive Director, University Audit and Advisory Services
David Jones, SR IT Auditor, University Audit and Advisory Services
Audit Results, Recommendations, and Responses

1. Privileged accounts are not consistently provisioned through exception accounts as required by the Privileged Account Standard.

**Condition:** Testing indicated that privileged access was not consistently provisioned to exception accounts. Specifically, privileged access was provisioned to non-exception accounts in 20 of the 42 servers reviewed involving 38 of the 95 (40%) associated accounts.

**Criteria:** ASU’s Privileged Accounts Standard requires privileged access to be provisioned to an exception account to ensure least privilege.

**Cause:** Exception accounts have not been consistently applied within the UTO. In a few instances, ids had been migrated to exception accounts; however, access granted to the standard account was not removed.

**Effect:** provisioning privileged access through standard accounts increases the risk of compromised credentials resulting in unauthorized access and other malicious activity. Testing involved servers that run key applications that have sensitive information.

**Recommendation:** Privileged access should be migrated to exception accounts as required by the Privileged Account Standard.

**Management Response:**

UTO agrees with the audit recommendation. UTO will clarify the scope in the Privileged Account Standard and investigate an enterprise supported tool to deliver efficiency and automate compliance. The exceptions noted will be corrected by December 31, 2020. The standard will be updated by March 31, 2021.

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

**Condition:** Servers are not logging system information as required but the System Audit Requirement Standard. In addition, 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 servers 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, was not functioning as intended due to an identified group policy conflict. Periodic reviews of logs are not occurring which would have identified that the group policy wasn’t working.

**Effect:** Testing identified that 33% (14 of 42) servers did not have audit logging running.

**Recommendation:** Resolve the identified Group Policy conflict where necessary. In addition, implement periodic reviews to validate that logging is occurring as intended which would have detected the Group Policy conflict.

In addition, further discussion of log retention should be held to ensure leadership is aware of the space limitation and accepts the risk of having logs for less than the required one year period.

**Management Response:**

UTO agrees with the audit recommendation. The group policy conflict was resolved October 5 2020. UTO will draft a strategy to deploy an event logging and monitoring tool for required systems. Reviews will be completed on a regular cadence. Logs will be retained for 12 months or a risk acceptance will be obtained from the accountable administrator. This will be implemented by June 30, 2021.

3. The UTO has implemented processes governing change management; however, further improvement is necessary to ensure planning components are considered and documented.

**Condition:** The UTO has implemented processes to follow the enterprise change management processes including utilizing the established process within Service Now; however, these processes do not consistently capture the planning components of the change.

**Criteria:** ASU’s enterprise change management process established a requirement for a formal change management process. It provides the framework that:

- Identifies the flow of activities, roles and responsibilities, and inputs and outputs of the ASU change process.
- Minimizes the impact of change-related incidents upon quality of servers and consequently improves day-to-day operations of the University.
- Establishes a formal process of recording, assessing, authorizing, scheduling and effectively communicating changes to ASU’s technology systems.
- Provides a framework for managing IT baseline configurations and changes for all
UTO-operated and managed devices.

- Ensures all changes have been properly assessed for their potential impacts to the ASU IT environment and a risk-based approval process is applied prior to implementation.
- Establishes processes for initiating, tracking and approving change requests.
- Clarifies specific roles, responsibilities and timelines related to change management.

**Cause:** UTO has implemented change management processes; however, do not follow them consistently as they relate to planning components to ensure all changes have adequate consideration and documentation.

**Effect:** Testing indicated that the existing processes are omitting key planning aspects of the change management process including change, back out, and testing plans which may impact UTO’s ability to adjust if the change does not go as intended. Specific testing identified that 36% of the changes reviewed (40 of 112) did not have the planning components of the change documented.

**Recommendation:** The University Technology Office should follow the defined change management process including ensuring all approved changes contain the necessary information to comply with the Enterprise System Change Management Standard.

**Management Response:**

UTO agrees with the audit recommendation. The standard will be updated to classify change types and define requirements. We have recently transitioned to a new ServiceNow module to enhance tracking and change management governance. Planning documentation (change, back out, and testing plans) will be required for appropriate (not all) change requests by June 30, 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
Lev Gonick, Chief Information Officer
Jess Evans, Chief Operating & Digital Transformation Officer / Interim Chief Information Security Officer
Nate Corwin, Executive Director
Nate Wilken, Senior Director Architect
Internal Audit Review Board
This page intentionally left blank