Arizona State University
Office of University Audits
Information Technology General Controls
Business and Finance
August 19, 2019

Summary: The Information Technology General Controls 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 for applications managed by Business and Finance. 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 Business and Finance. 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 seven high or medium risk departmental applications managed by Business and Finance. Applications chosen included applications that contained sensitive information such as student data, employee data, security data, and HIPAA data, as well as critical applications required to fulfill Business and Finance 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:

- 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 that safety-sensitive/security positions are appropriately restricted.
    - 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 application requires 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 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.
- 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 (COOP) accurately represent the departmental applications.

Conclusion: Overall, Business and Finance has implemented effective information technology controls related to encryption, logging and monitoring, backups, and vulnerability management; however, further improvement is needed to ensure controls are operating as intended in the areas of logical access, password complexity, and vendor oversight. It was also noted that the continuity of operations plans lacked accurate application data to ensure recovery.

Specifically, testing indicated that logical access was not appropriately restricted in four of the seven applications reviewed with exception rates ranging from 12% - 60%. In two of the applications, automated procedures were utilized to manage removal of access; however, processes were not working as intended resulting in access not being removed. Formalized access reviews were not in place, which would have detected the inappropriate access.

In addition, three of the seven applications reviewed did not meet the defined password complexity standards. In one instance, no password complexity had been established related to an application that stores sensitive employee information as well as HIPAA data. Excluding one application, necessary configuration changes were made during the audit to comply with requirements. In the remaining instance, the application owner is working with the vendor to implement the necessary changes to minimize the impact to the end users.

Business and Finance Information Technology (BFIT) has implemented processes to centralize the security review process; however, this process requires further enhancement to ensure all security reviews are being performed. In addition, processes have not been implemented to manage third party service provider oversight. As a result, none of the three hosted applications reviewed had performed the required oversight related to collecting and assessing SOC2 reports and required vulnerability scans.

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	7
• Logical access provisioned to a safety-sensitive or security position has a fingerprint background check on file with Human resources prior to access as defined by ACD126.	Opportunity for Improvement	1	7
• Password requirements and complexity configuration meet the defined Information Security Policy.	Opportunity for Improvement	2	9
• Encryption is implemented to meet the defined Data Handling Standard for data in transit.	Reasonable to Strong Controls in Place.	N/A	N/A
• Vulnerability management is implemented including review, analysis, and remediation as defined by the Web Application and Network Security Standards.	Reasonable to Strong Controls in Place.	N/A	N/A
• Logging and monitoring is implemented to meet the defined System Audit Requirements Standard.	Reasonable to Strong Controls in Place.	N/A	N/A
• Change Management is implemented to meet the	Opportunity for Improvement	3	10

defined Enterprise System Change Management Policy.			
• Patch Management is implemented to meet the defined Patch Management Standard.	Opportunity for Improvement	4	11
• Internal security reviews are in place to ensure technology purchases comply with ASU's Security Review requirements.	Opportunity for Improvement	5	12
• Third party vendor management oversight is implemented to ensure compliance with defined Security provisions.	Opportunity for Improvement	6	13
• Departmental applications are accurately reflected in the Continuity of Operations Plans.	Opportunity for Improvement	7	14
Compliance with Laws and Regulations	Not Applicable		

We appreciate the assistance of the Business and Finance 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 seven applications reviewed with exception rates ranging from 12%-60% (estimated). In two of these applications, exception rates are estimated due to the pervasive access issues noted with the application and the need to do a full detail review, which was not performed as part of our testing.

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

- Two applications had inappropriate administrator level access.
- Inappropriate generic accounts were in use in two of the applications.
- One application had access provisioned to individuals that are not ASU affiliates in violation of Access to University Technology Resources and Services Policy. This access was appropriate; however, should have been provisioned through the courtesy affiliate process. In addition, two other applications also included access provisioned to individuals that are not ASU affiliates. In these instances, we are not able to determine if the access is appropriate or not due to the pervasive access issues noted with these applications.
- One application requires individuals that have privileged access to be fingerprinted prior to access being provisioned. While processes have been developed to address this requirement, they are not being followed. Specifically, six of the 15 individuals tested did not have the required fingerprinting performed. None of the 15 selections had the required documentation based on the existing process.

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, ACD126 requires that safety-sensitive or security position pass a fingerprint background check prior to access provisioning.

Cause: For two of the applications, automated processes were utilized to facilitate access removal; however, these processes were not operating as intended resulting in access not being removed appropriately. For the other two applications, informal processes were in place, which were not effective.

Of the seven applications, only one had a formalized access review in place. As a result, inappropriate access is not being detected.

Effect: Access to the Business and Finance departmental applications is not appropriately restricted which may result in inappropriate or unauthorized access or changes to data.

Recommendation: Business and Finance should formalize access-provisioning processes for the applications that are handled informally including determining where existing processes can be leveraged to automate access removal. These processes should include ensuring compliance to ACD 125 related to provisioning access only to individuals that have a valid affiliation status. In addition, formalized access reviews should be implemented across all applications to ensure access is appropriately restricted.

Existing processes related to ensuring fingerprinting requirements should be reviewed with the respective teams to ensure a complete understanding of the requirement along with additional management oversight to ensure controls are being performed.

Management Response: The following remediation actions have been complete or are in process to address the inappropriate access. BFIT has direct ownership of the first two applications while business units within Business and Finance own part or all of the actions on the remaining two.

- Application 1: The automated script implemented was not running properly. The necessary corrections have been implemented and confirmed. In addition, all inappropriate access has been removed.

- Application 2: There was no business process nor rules surrounding who to remove and when. We scripted a manual method to remove all terms and implemented it (running it daily). BFIT is working with EHS to get approvals for the logic on offboarding expired affiliations (and requiring them to begin with) and automating both processes. This will be done by November 30, 2019.

- Application 3: This application has users added by the sub-administrators in the department (FDM). Prior to the audit, they had no method for removing inactive users nor were proper reviews being conducted. The one item that was providing some access control was the implementation of an expiration date for non-affiliates. Another point of concern was the use of generic accounts being used by third party vendors. FDM has worked to require nearly all such users to obtain their courtesy affiliations. There is one vendor that remains an exception to this, which is being vetted by GPIS. In addition, FDM has initiated a full access review of all users. All necessary actions are expected to be complete by January 2020.

- Application 4: This application is managed by the Preparedness and Security Initiative team. They have developed a detail action plan to address the access and fingerprinting issues noted. BFIT will provide oversight over this plan to ensure necessary actions are complete.

  Fingerprinting: The PSI team is developing a new user checklist that must be followed and updating the ServiceNow access request form to ensure the process is fully outlined. A full review of current users is being performed to identify who still requires fingerprinting. Individuals that still require fingerprinting will be initiated once the full review is complete. All items will be implemented by September 30, 2019.

  Access Provisioning: The PSI team has already requested to be added to the daily email regarding terminations and transfers. They are in process of developing and documenting the daily process to review listings and remove access. As part of this process, they will determine how to handle courtesy affiliate accounts. All items will be implemented by September 30, 2019.

In addition, periodic access reviews are being implemented across all applications to be performed at a minimum on an annual basis. Due to the initial access clean up that occurred at the time of the audit, the first time annual reviews will be performed as of June 2020.

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

Condition: Four of the seven applications reviewed did not meet the defined password complexity standards.

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)
- The account locks for 10 minutes after 25 incorrect password input attempts.

Cause: In three of the exceptions, the application has the ability to comply with the majority of the complexity requirements; however, were not configured correctly. Two of these are hosted applications managed outside of BFIT.

The remaining application that did not meet the requirements was due to a system limitation. To mitigate this system limitation, BFIT has implemented two-factor authentication to access the application.

Effect: Passwords do not meet the defined complexity requirements increasing the risk of potential compromised credentials resulting in unauthorized access. In one instance, no password complexity had been established related to an application that stores sensitive employee information as well as HIPAA data.

Recommendation: Business and Finance should update the existing configuration to meet the defined standard for internally managed applications. It is also recommended that additional processes be established to include appropriate oversight of implementing third party applications to ensure appropriate consideration is given to security configurations.

Management Response: Where possible, applications were brought into compliance during the audit. The application owner for the remaining application is working with the third party vendor and plans to implement additional complexity requirements by the end of August.

3. Business and Finance has implemented some processes governing change management; however, further improvement is necessary to ensure compliance with defined enterprise change management requirements.

Condition: Business and Finance has generally implemented various processes including the standard enterprise change management process within ServiceNow, as well as other processes utilizing various instances of JIRA; however, these processes do not capture all of the required components of the change management policy. In addition, one application tested did not follow any defined processes.

Criteria: ASU's enterprise system change management process establishes a requirement for a formal change management process. It provides a framework for

- 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 service and consequently improves the 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: Business and Finance has consolidated most information technology support to the centralized IT Team (BFIT) over the past several years. As a result, many of the applications tested were previously managed by the department themselves resulting in a variety of processes being followed. BFIT's focus has been primarily to ensure key risks are being addressed related to Change Management rather than ensuring compliance to the defined standard or standardizing processes across Business and Finance.

Effect: Testing indicated that existing processes around change management are generally being consistently followed for the various applications; however, these processes are omitting key aspects of the change management process including planning, assessing, authorizing, scheduling, and communicating changes.

Recommendation: Business and Finance should implement one standard method of change management across the environment. This will help minimize the variances that currently exist while at the same time shore up the missing components in the existing processes.

Management Response: For the non-vendor managed applications, this was consistently noted as an area in need of improvement. While BFIT is performing acceptable change management, these processes are not being formally documented in all cases. We first need to formally lay out the steps in our change management process and ensure that GPIS approves it. We then need to formalize the documentation process to include using a consistent tool for tracking communications and approvals as well as defining what changes should be in scope of such robust change tracking. This will be implemented by November 30, 2019.

4. Business and Finance has implemented some processes governing patch management; however, further improvement is necessary to ensure compliance with defined patch management standard.

Condition: Business and Finance has generally implemented some processes around patch management; however, the current process does not result in adequate

documentation to ensure appropriate process is being followed consistently and is not compliant with the defined patch management standard. In addition, one application tested did not follow any defined processes.

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. If testing shows patching is not feasible, mitigating controls should be implemented to prevent exploitation and should be communicated to the Chief Information Security Officer.

Cause: Business and Finance has consolidated most information technology support to BFIT over the past several years. As a result, many of the applications tested were previously managed by the department themselves resulting in a variety of processes being followed. BFIT's focus has been primarily to ensure key risks are being addressed related to patch management rather than ensuring compliance to the defined standard or standardizing processes across Business and Finance.

Effect: Testing indicated that existing processes around patch management are generally being consistently followed for the various applications; however, these processes are omitting key aspects of the patch management standard including planning, testing, approvals, notifications and capturing mitigating controls implemented for patches that are tested and found non usable. As a result, it is not known if patches are being assessed and applied in a timely manner.

Recommendation: Business and Finance should implement one standard method of managing patch management across the environment. This will help minimize the variances that currently exist while at the same time shore up the missing components in the existing processes.

Management Response: This will be a subset of the change management process implementation described in item 4, above. Patch application will be managed in the same fashion as any other changes.

5. Business and Finance has implemented a centralized process to ensure security reviews are performed over software purchases; however, further improvement is required to ensure reviews are performed and are accurate

Condition: Business and Finance has centralized responsibility for performing security reviews with BFIT; however, current processes do not ensure all software purchases are routed through this team to ensure reviews are performed.

Criteria: ASU Information Security requires that departments purchasing and implementing software and technology also implement appropriate security controls to safeguard university assets. Specifically, one of four levels of security reviews are required based on the data contained within the application and criticality to overall operations.

Cause: BFIT is not consistently involved in the purchasing activities related to software purchases. As a result, the required security review and related review of the risks the technology introduces are not always being appropriately assessed at time of purchase or subsequent renewals.

Effect: Two of the four purchases related to applications included in the review did not have the required security review performed.

Recommendation: Business and Finance should formalize internal purchasing activities to require BFIT involvement prior to technology purchases. This will ensure adequate visibility to potential security risks related to the purchase in addition to ensuring appropriate IT support and oversight exists from initial purchase and implementation.

Management Response: We are implementing new processes that will require departments to engage directly with the IT department prior to purchasing any BFIT related products. Most of the challenges have come from software purchases that are not being run through IT prior to decisions being made. The new process should route all needs through BFIT to ensure we have security reviews in place prior to purchases or commitments. This process will be fully implemented by November 30, 2019.

6. Business and Finance has not implemented appropriate vendor management processes over third parties to ensure compliance with required security provisions.

Condition: Business and Finance 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 business owner of the application is responsible for ongoing vendor management related to hosted third party software vendors. These individuals do not have appropriate visibility into the requirements of utilizing a third party vendor and are not currently collecting or assessment related SOC 2 reviews nor the required vulnerability/penetration scans for high and medium risk applications.

Effect: Vendor oversight processes have not been performed any of the three hosted applications included in this review. As such, none of the SOC 2 reports were collected or reviewed nor where the required vulnerability scans/penetration tests collected as required by the Web Application Security Standard.

Recommendation: BFIT should implement a centralized process to monitor and assess third party vendors. While this activity should involve the business owners, BFIT has the necessary technical knowledge necessary to perform an effective review and assessment of the third party vendors to ensure adequate visibility into the overall security risks.

Management Response: BFIT will maintain the overall inventory of applications utilized within Business and Finance along with the respective application owners. This will be utilized to track necessary actions with third party service provides including collecting and reviewing SOC reports and obtaining required security scan results as necessary.

7. Departmental applications are not accurately represented in the Continuity of Operations plans.

Condition: Business and Finance applications are not included in the respective Continuity of Operations plans (COOPs).

Criteria: Continuity planning includes the creation of a strategy to address both the threats and risks facing Business and Finance 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: Business and Finance Information Technology are not involved in the creation and updates of the Continuity of Operation plans.

Effect: With the exception of one application, departmental applications are not adequately captured in the COOPs resulting in a high risk of inability to achieve a timely restoration in the event of a disruption.

Recommendation: Business and Finance Information Tech owners should be involved with the annual update and review of the Continuity of Operation plans to ensure adequate information is captured to support recovery needs.

Management Response: This will require conversations with the functional owners of each application to ensure that they include these in their COOPs. BFIT technical administrators will work with the application owners to make sure they are included and that a feasible plan of action is agreed upon and in place should the COOP ever need to be executed. This will be complete by February 2020.

Distribution:

Arizona Board of Regents Audit Committee
Michael M. Crow, President
Morgan R. Olsen, Executive Vice President, Treasurer, and Chief Financial Officer
Kevin Salcido, Vice President Human Resources and Chief Human Resources Officer
Nichol Luoma, Associate Vice President, University Business Services
Rudy Bellavia, Managing Director and Chief of Staff, Office of Business and Finance
Jillian McManus, Executive Director Workforce Development, Human Resources
James Dwyer, Executive Director, Auxiliary Business Services
Allen Clark, Executive Director, Preparedness and Security Initiatives
James Nichols, Director BFIT, Business and Finance Support Services
Internal Audit Review Board