



Internal Audit Department

Access Management Audit

**October 2, 2020
Report Number FY 20-05**

Distribution:

Audit Committee, Arizona Board of Regents

Internal Audit Review Board

Rita Cheng, President

Steve Burrell, Chief Information Officer, Vice President, Information Technology Services

Pam Fleece, Director, Human Resources Information Systems

Bjorn Flugstad, Vice President, Finance, Institutional Planning and Analysis

Suzanne Hanks, Director, Service Desk & Technical Support Services

Kevin Hayes, Applications Systems Analyst, Enterprise Information Services

Terri Hayes, Executive Director, University Advising

Trey McCallie, Identity & Access Management Team Lead, Information Security Services

Michelle Parker, General Counsel

Jeremy Sanderlin, Associate Director, Strategic Planning, Implementation & Education Services

Andrea Stalker, Director, Strategic Planning, Implementation & Education Services

Wendy Swartz, Associate Vice President and Comptroller

PJ Way, Director, Infrastructure & Platform Services

Brett West, Associate Director, Infrastructure & Platform Services

Michael Zimmer, Director, Information Security Services

This report is intended for the information and use of the Arizona Board of Regents, NAU administration, the Arizona Office of the Auditor General, and federal awarding agencies and subrecipients.

This page intentionally left blank

Northern Arizona University
Access Management
Internal Audit Report
October 2, 2020

Summary

Audit of Access Management is in the Annual Audit Plan for Fiscal Year 2020, as approved by the Audit Committee of the Arizona Board of Regents (ABOR). This audit supports Northern Arizona University's (NAU / University) strategic goal of Stewardship by ensuring propriety of identifying, granting, and monitoring appropriate access to individuals, including compliance with applicable laws, rules and regulations.

Background: Identity and Access Management (IAM) is the process used in businesses and organizations to grant or deny employees and others authorization to secure systems¹. IAM processes are used to initiate, capture, record, and manage user identities and related access permissions to the personal, protected, and proprietary information managed by systems and processes owned or leased by NAU. The IAM program and its related services² are responsible for managing faculty, administration, and student information; access to NAU applications and information; and the distribution of information to external parties. NAU's information technology environment was organized as a decentralized structure until 2016 when centralizing the environment was initiated to improve resource utilization, service delivery, data security and regulatory compliance. As such, while Information Security Services (ISS) has ultimate responsibility for managing the University's IAM program, IAM cross-functional activity still involves several NAU departments. For additional details, including the identity lifecycle, NAU's Information Security Program governance structure, and access reviewed for this audit, see Exhibit A.

The business processes and supporting technologies attempt to address:

- Who has access to what information?
- Is the access appropriate for the task being performed?
- Is the access and activity monitored, logged, and reported appropriately?

Audit Objective: To ensure user access management is appropriate and adequate, including physical access, logical access and identity verification, for NAU systems and related data.

Scope: The overall purpose of the audit is to report on the identity and access management controls and processes established by the University to provide the right people with the right access at the right time. The scope included a review of all policies, procedures and practices governing identity and access management, including review of documents and system reports supporting compliance and reporting requirements during the 2018-2019 Academic Year and / or through Spring 2020. We did not test individual system / application access controls for all of NAU's many information technology systems but instead focused on the review of access controls for one high profile system, Salesforce, as well as the Lenel system as it relates to supporting access to NAU's data centers. We conducted such analysis, tests and other procedures as we deemed necessary to address the audit objective.

Methodology: The following procedures were performed to accomplish the audit objective:

- Reviewed current and draft policies and procedures related to NAU's Information Security, Affiliates, and Access Management.

¹ Definition – What does *Identity and Access Management (IAM)* Mean? Retrieved from <http://www.techopedia.com/definition/23922/identity-and-access-management-iam>

² Identity and Access Management's related services include password management, authentication and authorization systems, user lifecycle management, privileged access management, incident response, guidance for complying with IAM controls, oversight of IAM activities, and other related services. Northern Arizona University, *Access Management Policy* (2019).

Northern Arizona University
Access Management
Internal Audit Report
October 2, 2020

- Reviewed meeting minutes of the governing committee and trustees.
- Reviewed Arizona Revised Statutes (ARS) and ABOR information technology security policies.
- Reviewed National Institute of Standards and Technology (NIST) guidance to identify best practices related to identity and access management, physical access and user authentication.
- Interviewed ITS, NAU Police Department, Utility Services, Campus Services & Activities (CSA), and American Campus Communities staff to understand existing processes, including procedures for managing affiliate accounts, access to physical structures, Salesforce logical access, identity verification, and local privileged accounts.
- Reviewed and analyzed user accounts and settings to determine if access is appropriate for tasks, is properly approved and provisioned, is adequately monitored, and is timely revoked.
- Obtained server inventory lists from the Comptroller, Property Surplus, and the Enterprise Reporting System ITS Asset Listing to determine the quantity and location of physical servers, and that all such critical technology is identified.
- Toured the University's wiring closets, utility tunnels, secure data centers, and server rooms and American Campus Communities' intermediate and main distribution frame rooms.
- Reviewed access logs for individuals associated with the University to determine if access to data centers is adequately monitored and secured.
- Reviewed local administrator accounts and activities to determine how to minimize / monitor usage.

The audit was conducted in accordance with the *International Standards for the Professional Practice of Internal Auditing promulgated by the Institute of Internal Auditors* and accordingly, included such tests considered necessary under the circumstances.

Conclusion:

Controls Assessed		
1	13	2

Overall, the University has implemented reasonable, risk-based processes for ensuring access is limited to the right people with the right access at the right time. Risk-based control approaches are also in place to manage the resources available for protecting the network and physical environments. Implementing an enterprise-wide identity and access management (IAM) system would provide the best value to NAU in terms of providing centralized governance over IAM. An IAM system would automate various IAM activities (e.g., account provisioning / de-provisioning, etc.), decreasing organizational risk and increasing productivity by providing a predictable and consistent mechanism to enable restricting administrative access, thereby ensuring the right attributes would be automatically provisioned to a target system. Given the current budgetary challenges, procuring such a system in the immediate or short-term is not feasible and therefore not a solution. As such, ITS has implemented a variety of key processes in this regard, which could be improved by:

- Implementing the current draft Affiliates Policy and draft Access Management Policy and standards to be applied across the NAU Community.
- Enhancing the routine monitoring of accounts, privileges, and access to provide additional assurance that systems are securely safeguarded.
- Updating technology documentation, including the server inventory, using existing NAU tools and technologies to help ensure the complete University physical infrastructure is properly managed, monitored, and protected from internal and external threats.

Identity and access management policy, procedure and practice appear to be improving as IT centralization matures. Focused attention on resources; skills development; and technologies that

Northern Arizona University
Access Management
Internal Audit Report
October 2, 2020

automate processes to yield increased efficiency, accuracy and timeliness are critical to ensuring NAU's continued success in protecting NAU systems and data.

Observations: We noted the following observations:

- ISS applies a risk-based approach to oversight and management of identity and access management in line with the NIST Cybersecurity Framework to help ensure resources are focused on the most significant threats.
- Draft Affiliates and Access Management policies and standards are currently in progress.
- Unique user accounts are auto generated and appear to be assigned appropriate permissions and profiles.
- Established Electronic PeopleSoft Administrative Security System (ePASS)³ processes provide additional security and management of access to key systems like PeopleSoft and Salesforce.
- Identity verification conducted by functional areas on NAU's main campus is being improved by developing processes in accordance with NIST standards.

We identified improvement opportunities related to access management standards development, affiliate account management, proper safeguarding of data centers, Salesforce user account provisioning utilizing the ePASS process, standardizing identity verification processes, and local administrator account monitoring, for which management is implementing solutions as identified in this report. The control standards considered, related control environment assessment and any related improvement opportunities identified are summarized 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/ Assessment	IO No.	Page No.
Safeguarding of Assets:			
• Identity Verification: User identities are properly validated before allowing transactions having information security implications, including modifying or communicating any authentication credentials.		10	15
• Logical Access & Identity Verification: Requests to create or modify accounts and access privileges are documented and approved by the requestor's supervisor and the data / system owner before access is granted.		4	9
• Logical Access: All user accounts and privileges are routinely monitored and timely disabled and / or revoked.		2, 3, 8, 11	6, 7, 13, 17
• Logical Access: Automated controls exist to disable passwords and deactivate orphan accounts within a specified period.		1	5
• Logical Access: Each user is assigned a unique account.			
• Logical Access: Only approved users have access to University data.		4	9
• Logical Access: Privileged administrator level account access is assigned only to users specifically requiring such access.			
• Physical Access: Climate controls are deployed in data centers and operate sufficiently.		6	11

³ The Electronic PeopleSoft Administrative Security System (ePASS) is an electronic form within NAU's PeopleSoft LOUIE system that allows for paperless administrative security requests and security revocation. Retrieved from <http://www.in.nau.edu/its/epass>

Northern Arizona University
Access Management
Internal Audit Report
October 2, 2020

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/ Assessment	IO No.	Page No.
<ul style="list-style-type: none"> Physical Access: Level access is monitored and managed efficiently and effectively to ensure unauthorized physical access to data centers is minimized. 		9	14
<ul style="list-style-type: none"> Physical Access: Physical controls are in place to ensure only the intended cardholder account can use assigned badges to gain access to data centers. 		7, 8	12, 13
<ul style="list-style-type: none"> Physical Access: Servers are routinely inventoried to ensure proper and secure safeguarding. 		5	10
<ul style="list-style-type: none"> Physical Access: Video monitoring exists to ensure only approved users with access are entering data centers. 		5	10
Effectiveness and Efficiency of Operations:			
<ul style="list-style-type: none"> Logical Access: Automated controls exist to disable passwords and deactivate unused accounts within a specified period. 		1	5
<ul style="list-style-type: none"> Physical Access: Automated systems exist to manage and monitor data center access. 		7	12
Compliance with Laws and Regulations:			
<ul style="list-style-type: none"> Logical & Physical Access: NAU policies and procedures exist to identify and disable user accounts for transferred and / or terminated employees. 		1, 3, 8	5, 7, 13
<ul style="list-style-type: none"> Logical & Physical Access, & Identity Verification: NAU policies and procedures exist to ensure access to systems or data is controlled through use of standardized identification and authentication mechanisms. 		1, 10	5, 15

Legend:	
Reasonably Strong Controls In Place	
Opportunity for Improvement	
Significant Opportunity for Improvement	

We appreciate the assistance and cooperation provided by ITS Information Security Services staff, ITS Enterprise Information Services staff, ITS Infrastructure & Platform Services staff, ITS Strategic Planning, Implementation & Education Services staff, Utility Services staff, NAU Police Department staff, Campus Services & Activities Administration staff, and American Campus Communities staff.



Robin Mosness, MS, MS
Senior Internal Auditor
Northern Arizona University
(928) 523-6459
robin.mosness@nau.edu



Karletta Jones, CPA, CIA
Senior Internal Auditor
Northern Arizona University
(928) 523-4136
karletta.jones@nau.edu



Mark P. Ruppert, CPA, CIA, CISA
Chief Audit Executive
Northern Arizona University
(928) 523-6438
mark.ruppert@nau.edu

Audit Results: Improvement Opportunities & Solutions

1. Implementing the draft Access Management Standards for all University users, systems, applications, and networks could better define expectations and standardize routine procedures throughout the NAU Community.

Solution: The Access Management Standards draft document will be reviewed and updated to include core standards applicable to all University departments and functions conducting common access-related activities. The Access Management Policy and Standards will be finalized and communicated through the University Policy Management processes by the end of December. However, a formal Access Management framework and implementation across the entire NAU Community will likely take a number of years to mature depending on various constraints including additional resources invested in organization, talent, and technological advancements.

Responsible Parties:

Michael Zimmer, Director, ISS
Trey McCallie, IAM Team Lead, ISS

Implementation Date:

12/31/2020

DETAILS:

Condition: The NAU Information Security Services Identity and Access Management (IAM) program consists of four employees who ensure that access to the University's information technology network is operating efficiently and securely. These employees focus their efforts primarily on the centrally managed IT environment, including the NAU student facing network. However, identity and access management responsibilities consist of automated and manual processes decentralized across the University as follows:

- Affiliate account access is managed by Strategic Planning, Implementation & Education Services (SPIES).
- Physical access is managed by Facility Services, ITS Infrastructure & Platform Services, Campus Services & Activities, and NAU Police Department.
- Access to Salesforce is managed by ITS Enterprise Information Services, Salesforce Administration Team.
- Identity verification or authorization is conducted by at least eight functional areas on the main campus (see additional details at IO 10).
- Local administrator accounts on University-owned personal computers are managed by ITS Service Desk & Technical Support Services.

The current draft Access Management Standards document provides guidance for standard and privileged account access; however, it excludes standards addressing account provisioning and de-provisioning, password controls, authentication controls, access recertification controls, and inactive account controls. Updating and implementing the policy and standards would increase assurance regarding the consistency of such practices throughout the NAU community.

Audit Results: Improvement Opportunities & Solutions

Criteria: Standards define ways of working to achieve the objectives of the organization. Adopting and enforcing standards promotes efficiency and ensures consistency in the IT operating environment⁴.

Cause: Due to the decentralized environment, much of the responsibility for controlling access to University data is at the division level, which is not formalized or consistently managed. While the Access Management Policy and Standards are drafted and were most recently reviewed in Spring 2020, the policy remains incomplete due to competing priorities exacerbated by COVID-19 as well as the need for ample resources to support policy enforcement once implemented.

Effect / Impact: Consistency in process and expectations for responsibilities could be compromised resulting in inappropriate access, data breach, customer dissatisfaction, and inability to support an effective monitoring and compliance process.

2. Affiliate account management could be improved by evaluating and updating affiliate account settings to comply with NAU policies and procedures.

Solution: As of June 2020, affiliate accounts were reviewed and evaluated for compliance with the ITS Affiliate Policy. Affiliate account expirations were reset based on affiliate type per established business rules with no expirations exceeding 60 months. The Affiliate Request Form and Affiliate Policy will be updated to remove the required social security number data element.

Responsible Parties:

Mark Niles, Systems Analyst, Sr., SPIES
Trey McCallie, IAM Team Lead, ISS

Implementation Date:

12/31/2020

DETAILS:

Condition: Affiliate accounts are used to provide authorized access to a variety of individuals who are not current and active NAU employees or students. Such individuals include consultants, vendors, NAU retirees, NAU emeritus professors, etc. While account provisioning is assigned to a specific ITS employee, the accounts are not actively monitored to ensure compliance with related NAU policies and procedures. In this regard, the following areas for improvement were identified:

- Although required in policy, clear University business needs are not defined or documented in the affiliate request process, but rather implied by virtue of having an affiliate sponsor.
- Per the ITS Affiliate Policy, affiliate account expirations are not to exceed 60 months. From the raw data export file of active affiliates as of 1/23/2020, we observed 932 affiliate accounts with expiration dates between 2025 and 2041. We observed that 1,027 affiliate accounts have blank Last Password Change fields, indicating users have either not accessed these accounts or have not renewed passwords.

⁴ Mar, S., Johannessen, R., Coates, S., Wegrzynowicz, K., & Andreesen, T. (2012, March). Information Technology Risk and Controls [PDF file]. *Global Technology Audit Guide*, 2, 18. Retrieved from chapters.theiia.org/montreal/ChapterDocuments/GTAG

Audit Results: Improvement Opportunities & Solutions

- The current policy and request form require affiliates to provide social security numbers, which are not necessary for provisioning these accounts.

Criteria: The current Affiliate Policy states, “There shall be a clear University business need established before any computer accounts are issued. Simply desiring an email account in order to communicate with NAU counterparts is not a sufficient reason to establish an affiliation with NAU.” The Affiliate Policy also provides a default service period of 12 months (or shorter upon request) and no greater than 60 months. ITS Self Service – Passwords provides Maximum Password Age settings providing criteria as, “...the amount of time (in days) that a password can be used before the system requires the user to change it. The value has been set at 90 days for faculty and staff and anyone who has received FERPA privacy training. All others, mostly students, will have 120 days.”

Cause: Affiliate account management is the responsibility of an individual who was promoted into a new role but has maintained and improved the process despite having additional tasks. As a result, affiliate accounts management has not received the priority, resources and time necessary to routinely and completely support related policy requirements.

Effect / Impact: Unused accounts can create opportunities for system compromise by internal and / or external parties.

3. Requiring all Salesforce profiles to route through the ePASS security request system could help ensure roles are properly revoked upon user transfer or termination, thereby reducing the risk of system compromise through unused privileged accounts.

Solution: Pending implementation of the Salesforce Connected Campus Release 3 scheduled for calendar year 2020, a new University Advisor (UNIV_ADV) role will be created in the ePASS to ensure automatic notifications are sent to the Salesforce Administration Team when users having this role transfer or terminate employment. As part of the scheduled release, the Salesforce Administration Team will coordinate with University Advising to update procedures requiring employees to request the NAU_CRM_Oversight Support role and / or UNIV_ADV profile through the existing ePASS.

Responsible Parties:

Implementation Date:

Terri Hayes, Executive Director, University Advising
Kevin Hayes, Application Systems Analyst, Enterprise Information Services
Jeremy Sanderlin, Associate Director, SPIES

12/31/2020

DETAILS:

Condition: Account provisioning for the Salesforce system is handled by the Salesforce Administration Team. The Salesforce NAU_CRM_Oversight Support role is one of four available Salesforce proxy roles. Users assigned the NAU_CRM_Oversight Support role have the most

Audit Results: Improvement Opportunities & Solutions

responsibility for editing fields in Salesforce and the most reporting and dashboard functionality. The Salesforce UNIV_ADV profile is a separate profile assigned to advisors who need access to the University advisor dashboard within Salesforce. If users have the NAU_LS Advisor role assigned in PeopleSoft, they can request the Salesforce UNIV_ADV profile by creating a ServiceNow ticket or via email. If users have access to Salesforce, profiles are changed by the Salesforce Administration Team. If users do not have access to Salesforce, profiles are changed as requested; however, the Salesforce Administration Team also requests users create a security request through ePASS. There is currently no requirement to use ePASS and no follow-up to ensure a security request was created through ePASS for this group of users. Because electronic notification is provided through ePASS, when these users transfer or terminate, the Salesforce Administration Team does not receive notification of their actions. Salesforce permissions and / or profiles are not timely revoked, allowing users to access systems after transferring or terminating employment from the University.

A review of Salesforce accounts existing as of April 23, 2020 disclosed 21 out of 1,198 users, identified by employee ID (EMPLID), had active Salesforce roles after terminating from the University, including:

- One user with an elevated System Administrator (SYS_ADMIN) profile, which allows full system access; and
- Two users logged in to Salesforce up to two years after employment terminated. There was no indication of inappropriate activity identified in relation to these logins, their log-in profiles included no access to protected data, and the accounts were de-provisioned once identified.

Criteria: Managing Security for the Salesforce Customer Relationship Management (CRM) Implementation – Phase II⁵ states, “The PeopleSoft Security Administrators on the Change Management Team in ITS will be able to assist the Salesforce Administration team in complying with the University’s “access to data based on need” policy and the State Auditors directive that NAU procedures ensure a “timely revocation of administrative access to data” by performing the following reviews on a biweekly basis:

- Evaluate all users who are assigned administrative security roles in the PeopleSoft enterprise systems (which includes the Salesforce CRM proxy security roles) to ensure that their affiliation with the University is active, and
- Evaluate employees who change positions within the University to ensure that any administrative access held is still aligned with the new job responsibilities.

When a Salesforce proxy role is revoked as an outcome of these biweekly evaluations, an email will be generated from the ePASS system notifying the Salesforce Administration team that access to Salesforce should be discontinued.”

⁵ The Phase I Salesforce CRM implementation included populating the Salesforce Service Cloud with a full complement of bio demographic data extracted from PeopleSoft Campus Solutions. The Phase II Salesforce CRM implementation expanded the data accessed through the Salesforce CRM system to include student information from the administrative areas of Student Records, Student Financials, and Financial Aid. *Managing Security for the Salesforce CRM Implementation – Phase II, Revised October 2016, p. 1.*

Audit Results: Improvement Opportunities & Solutions

Cause: The Salesforce Administration Team relies on systems and users to provide notification of changes in status.

Effect / Impact: Users having access to systems without proper authorizations and approvals could unknowingly expose the University to risks associated with unauthorized access, such as data compromise and related regulatory compliance issues.

4. Developing a process for onboarding consultants to include timely completion of user account approvals through ePASS could ensure SYS_ADMIN roles are properly verified and synchronized with Salesforce permissions and profiles.

Solution: Pending implementation of the Salesforce Connected Campus Release 3 scheduled for calendar year 2020, all users, including affiliates, will require approval through ePASS prior to granting system access. If account provisioning is required prior to processing through ePASS, documented management approvals will be obtained by the Salesforce Administration Team.

Responsible Parties:

	Implementation Date:
Garrett Gallegos, Application Systems Analyst, Enterprise Information Services	
Kevin Hayes, Application Systems Analyst, Enterprise Information Services	12/31/2020
Jeremy Sanderlin, Associate Director, SPIES	

DETAILS:

Condition: When consultants are hired by the University, department hiring managers are responsible for ensuring user account requests are processed through the ePASS prior to providing access to University systems. Due to ePASS routing and approval delays, consultants hired under contract are sometimes provided immediate access to Salesforce without required approvals and security roles assigned in PeopleSoft. Two affiliate consultants had elevated SYS_ADMIN profiles assigned in Salesforce without corresponding ePASS approvals.

Criteria: Managing Security for the Salesforce CRM Implementation – Phase II states, “It will be very important to keep user access in the Salesforce system synchronized with the PeopleSoft HCM security system of record. When an individual is provided access to Salesforce, the individual must already have the requisite proxy security role assigned in the PeopleSoft security system of record. When an individual’s access to Salesforce is removed, the corresponding proxy security role in the PeopleSoft security system of record must also be revoked.”

Cause: A process does not exist for ensuring requested user access is approved through ePASS for all users prior to Salesforce account provisioning. Consultants are set up as affiliates; however, the Salesforce Administration Team is not provided timely information prior to consultant start dates and is authorized to allow Salesforce access, thereby overriding existing controls.

Northern Arizona University
Access Management
Internal Audit Report
October 2, 2020

Audit Results: Improvement Opportunities & Solutions

Effect / Impact: Affiliates having access to systems without proper authorizations and approvals could unknowingly expose the University to the risk of unauthorized access and audit compliance issues.

5. Server inventory should be identified and maintained based on a structured Secure Data Center layout to ensure systems and data are properly safeguarded.

Solution: A secure data center map will be created that identifies physical server inventory as well as additional safeguards that exist in protecting those physical servers. Additionally, an efficient and effective inventory tracking process will be identified to ensure server inventory is accurately and completely maintained.

Responsible Parties:

PJ Way, Director, Infrastructure & Platform Services
Brett West, Associate Director, Infrastructure & Platform Services

Implementation

Date:
12/31/2020

DETAILS:

Condition: A formal secure data center map does not exist. Facility mappings of IT buildings exist in Lenel but are outdated and include buildings that are no longer part of the IT segment.

While the majority of servers identified are in service, there are also many that are: Not In Use, Powered Off or were Not Known. While several ITS staff are designated as custodians for respective servers, there does not appear to be an effective and efficient process to ensure that server inventory is accurate and complete. The following table shows the details related to identified physical server inventory as of February 29, 2020:

	In Use	Not In Use	Powered Off	Unknown	Total
Maintained in ITS	\$ 3,875,773	\$ 71,214	\$ 341,425	\$ 841,008	\$ 5,129,419
Not Maintained in ITS					
Bldg 19 - Physical Sciences				8,206	8,206
Bldg 56 - Applied Research & Development				16,557	16,557
Bldg 16 - Communication	51,158				51,158
Bldg 54 - University Central Admin				11,272	11,272
Bldg 69 - Environment Forestry & Natural Sciences	48,935				48,935
Bldg 98A - NAU Police Department	15,722				15,722
	<u>\$ 3,991,589</u>	<u>\$ 71,214</u>	<u>\$ 341,425</u>	<u>\$ 877,042</u>	<u>\$ 5,281,270</u>

Chart Notes:

- All costs represent capitalized costs.
- In Use represents servers in use and powered on.
- Not In Use represents servers powered on but not in use.
- Powered Off represents servers not being used.
- Unknown represents servers for which insufficient information was available at the time the data was collected.
- Building 69 servers have been moved to Building 54 as of June 2020.

Audit Results: Improvement Opportunities & Solutions

Criteria: The Secure Data Center Physical Security Policy states, "Section 1.1 - Approved IT facilities include, but are not limited to, Secure Data Centers, Premises Wire Distribution Closets, and wall-mounted telecommunication cabling racks. A Secure Data Center is a University managed facility for housing computer, data storage, and / or network equipment that is protected with restricted physical access, environmental controls, power protection, and network firewalls. Section 1.2 - The Chief Information Officer must approve all IT facility locations and must ensure that each IT facility is appropriately kept safe, secure, and protected from physical harm and unauthorized access. Facility management officials must consult with the Chief Information Officer regarding any plan or action that may impact installed or planned IT facilities or the sensitive resources they contain."

Further, Sections 6.1 and 6.2 of the Secure Data Center Physical Security Policy speak to the deliveries and removals of equipment: "All Secure Data Center deliveries must be pre-authorized and documented. Equipment may only be moved or removed with prior authorization from the Secure Data Center manager. Disposal of equipment must occur in accordance with the University's Data Handling Protocols and all other applicable disposal / destruction requirements. Documentation of all disposal and destruction activities is mandatory and must include data, time, asset inventory number, and all system information including the data store."

Cause: A secure data center map is not currently deemed a priority. Several individuals are responsible for overseeing servers and due to performance and department needs, servers are maintained in secured ITS building spaces as well as other main campus building secured spaces.

Effect / Impact: Equipment inventory may not be correct, which could result in the misuse or underutilization of resources and / or compromise the integrity and availability of information maintained on those servers.

6. Updating security and climate monitoring of data center space would improve the security and longevity of related IT infrastructure.

Solution: As of May 2020, video surveillance has been installed and is fully operational at the South Node. As of June 2020, servers previously not maintained in ITS are now maintained in ITS. This has allowed two air handlers to become available that were used in those locations. The two available air handlers will now be installed in the North Node to correct the existing failing air handlers.

Responsible Parties:

PJ Way, Director, Infrastructure & Platform Services
Brett West, Associate Director, Infrastructure & Platform Services

Implementation Date:

Implemented 5/31/2020 -
South Node Camera
Implemented 9/30/2020 -
North Node HVAC Repairs

Audit Results: Improvement Opportunities & Solutions

DETAILS:

Condition: There are two main data centers on the NAU Mountain Campus, which includes the North Node. The North Node houses PeopleSoft production applications used by the University for financial activity, student activity and human resources activity. The data center in the North Node, while ultimately secure, has failing air handlers.

The South Node is a network and telecommunications systems node. This node does not house servers. The South Node does not have video surveillance.

Criteria: Section 4.1 related to Monitoring in the Secure Data Center Physical Security Policy states, "Video monitoring must be employed to record entry and exit of all individuals at all times."

Section 5.3 related to Emergency and Climate Controls in the Secure Data Center Physical Security Policy states, "Temperature and humidity controls must be deployed in all Secure Data Centers and server rooms."

Cause: Funding limitations delayed improvement until new opportunities were identified.

Effect / Impact: Monitoring is not available which could result in a data breach and climate controls could potentially cause damage to the servers housed in the North Node resulting in lost data that is critical to the University's operations.

7. Data center access approval and related workflow could be automated to allow for more efficient and effective review and approval related to initial and renewal data center access requests.

Solution: The data center access form will be routed through OnBase with the corresponding renewal also automated to allow for efficient and effective review and approval. An established review process will be maintained that includes OnBase reporting in conjunction with term reports, where applicable.

Responsible Parties:

PJ Way, Director, Infrastructure & Platform Services
Brett West, Associate Director, Infrastructure & Platform Services

Implementation Date:

12/31/2020

DETAILS:

Condition: Control over access to NAU's data centers appears to be generally well-controlled. However, the data center access form used to request and document approval of access is a hard-copy form requiring manual review and approval. The annual review of the form is also a manual process. Automating these processes can improve efficiency and reduce related paper processing costs. Automation may also help keep authorized access current as we noted:

Audit Results: Improvement Opportunities & Solutions

- Up until May 2020, Facility Services and the NAU Police Department staff were not required to complete an access request form.
- A data access form that was approved by a former employee is still being used as documentation to support approval for data center access by a NAU Foundation employee.

Criteria: Section 2 related to Secure Data Access Controls in the Secure Data Center Physical Security Policy states, “2.1. Restricted access to Secure Data Centers will be maintained by employing a formal, documented process to authorize entry only by appropriate personnel. 2.2. The Secure Data Center manager will maintain up-to-date lists of all personnel authorized to access Secure Data Centers and will review these lists quarterly to ensure their accuracy and completeness. 2.3. Access privileges for individuals who change roles or depart the University will be immediately terminated with all such changes carefully documented. 2.4. In accordance with federal regulations (NIST 800-53), access to approved IT facilities where classified information is stored must be carefully restricted to only authorized individuals.”

Cause: Competing priorities and lack of resources in time have resulted in continued use of the manual review and approval process.

Effect / Impact: Access by unauthorized individuals might not be identified timely.

8. Review of the employee termination report could be updated to include terminated student employees to ensure all potential Lenel cardholders and users are reviewed for employment changes.

Solution: Pam Fleece, Director, Human Resources Information Systems (HRIS), will provide updated term reports that will include termed student employees to Brett West. This will run on the same pay period cycle as the existing term report Brett uses in his review.

Responsible Parties:

Pam Fleece, Director, HRIS

PJ Way, Director, Infrastructure & Platform Services

Brett West, Associate Director, Infrastructure & Platform Services

Implementation

Date:

Implemented
9/22/2020

DETAILS:

Condition: Term reports are reviewed each pay period to ensure only authorized users have and continue to have access to data centers using the Lenel system; however, the existing term report does not include termed student employees.

Criteria: Section 2 related to Secure Data Access Controls in the Secure Data Center Physical Security Policy states, “2.1. Restricted access to Secure Data Centers will be maintained by employing a formal, documented process to authorize entry only by appropriate personnel. 2.2. The Secure Data Center manager will maintain up-to-date lists of all personnel authorized to access Secure Data Centers and will review these lists quarterly to ensure their accuracy and completeness. 2.3. Access privileges for individuals who change roles or depart the University

Audit Results: Improvement Opportunities & Solutions

will be immediately terminated with all such changes carefully documented. 2.4. In accordance with federal regulations (NIST 800-53), access to approved IT facilities where classified information is stored must be carefully restricted to only authorized individuals.”

Cause: Student separations were not included in the terminated employee report prepared by Human Resources.

Effect / Impact: The potential for a data breach exists due to data centers not being properly safeguarded by timely identification of unauthorized access.

9. Reviewing and updating Lenel system access management processes would help to ensure the most efficient and effective processes are implemented for review and approval of cardholders and users.

Solution: As of May 2020, the CIO has discussed the benefits of centralizing oversight of Lenel administration with Capital Planning and Campus Operations leadership. Additionally, the Lenel stakeholder group has been notified and these items are being discussed as part of the group’s goals. Automated provisioning / de-provisioning is in place and working successfully. Where applicable, requests will be made to the Lenel vendor for assistance. An NAU Lenel Administrator will be identified in the interim. Policies and procedures will also be developed and / or updated to include:

- Policy for access to high security areas:
 - Identification of high security areas,
 - Ownership of access levels associated with high security areas, and
 - Frequency of reviewing access levels for these areas.
- Policy for regularly scheduled reviews of access by segment administrators, which should also consider obtaining the most appropriate term report.
- Policies / processes regarding automatic system updates (addition and removal of users / badges by affiliation).

Responsible Parties:

PJ Way, Director, Infrastructure & Platform Services
Brett West, Associate Director, Infrastructure & Platform Services

Implementation Date:

12/31/2020

DETAILS:

Condition: The Secure Data Center Manager is tasked with overseeing and managing the Lenel system. Two Lenel groups, comprised of NAU campus-wide employees, exist to help with the endeavor of maturing the Lenel system from just a building access system to a true campus life / property safety system. The Lenel Users Group is intended for segment admins to learn and discuss the use of the Lenel system in their buildings for day-to-day purposes. The Lenel Stakeholder group develops standards and policies for equipment use, monitoring standards and emergency response guidelines. The following were noted as part of the review of the Lenel system:

Audit Results: Improvement Opportunities & Solutions

- A designated Lenel administrator does not currently exist to monitor and ensure campus-wide segment administrator reviews are performed and adequate and timely training is provided.
- Access level reports are not accurate.
- Existing safeguards and processes are not periodically evaluated to ensure the access or access removal is appropriate and timely.
- Periodic reports that identify unusual trends are not set-up in Lenel.
- Badging in and out of secure IT locations is required in some but not all locations and monitoring of such access is inconsistent.
- As a best practice, use of number pads as a multifactor entry requirement is not evident in these IT locations or any other area deemed secure on campus.
- The Lenel system logs do not provide enough information to accurately track user / cardholder status.
- Vendors, affiliates, and any special groups are not defined with corresponding guidelines and expectations in the existing Lenel policies and procedures.

Criteria: Section 2 related to Secure Data Access Controls in the Secure Data Center Physical Security Policy states, “2.1. Restricted access to Secure Data Centers will be maintained by employing a formal, documented process to authorize entry only by appropriate personnel. 2.2. The Secure Data Center manager will maintain up-to-date lists of all personnel authorized to access Secure Data Centers and will review these lists quarterly to ensure their accuracy and completeness. 2.3. Access privileges for individuals who change roles or depart the University will be immediately terminated with all such changes carefully documented. 2.4. In accordance with federal regulations (NIST 800-53), access to approved IT facilities where classified information is stored must be carefully restricted to only authorized individuals.”

Cause: Competing priorities and the shift to use the Lenel system as a campus life safety system in addition to secure data center access, which requires specific strategy and analysis, has delayed best practices and a solid process of review and approval in the campus-wide use of the Lenel system.

Effect / Impact: The potential for a data breach exists due to data centers not being properly safeguarded by timely identification of unauthorized access.

10. Establishing University-wide guidelines for authenticating individuals who request access to NAU systems or who have forgotten their access credentials will help ensure that authentication processes are sufficiently robust and consistent to protect NAU systems and related corporate, student, faculty and staff data.

Solution: As part of ISS continued focus on maturing IT security practices, ISS has established an Identity and Access Management Working Group and will develop identity verification / user authentication guidelines guided by NIST and applied across NAU that address:

Audit Results: Improvement Opportunities & Solutions

- Where knowledge-based authentication should be applied.
- Minimum number of authenticators that must be confirmed before granting or renewing access.
- Nature of type of authenticators deemed acceptable.
- Procedure documentation requirements.
- Authenticator documentation requirements.
- Nature of employees permitted and / or training / oversight required to apply such procedures.
- Training requirements.
- Oversight and monitoring requirements.

Responsible Parties:

Michael Zimmer, Director, ISS
Trey McCallie, IAM Team Lead, ISS

Implementation Date:

12/31/2020

DETAILS:

Condition: We identified eight functional areas on the main NAU campus that handle some level of identity authentication for individuals claiming to not know or have their system access credentials for the systems used by these areas:

- Cline Library
- EMSA Gateway Student Success Center
- Financial Aid
- ITS Student Technology Center (Tier 1)
- Registrar's Office
- Residence Life / University Housing
- ITS Student Technology Center (Tier 2) / ITS Help Desk
- JacksCard Office

While all areas applied some level of formal verification process, there is no consistency in how those procedures are applied. Of these areas:

- 4 Have not documented their verification process
- 2 Do not train those who handle the verification
- 6 Do not monitor those who do the verification
- 7 Permit student employees to verify IDs
- 3 Require 3 authenticators
- 3 Require 2 authenticators
- 2 Require 1 authenticator
- 7 Do not document the authentication applied to each request

A variety of authenticators are in use among the eight areas, including:

Audit Results: Improvement Opportunities & Solutions

Name?	8	Phone Number?	1
Student ID Number / EmplID?	6	Account Access Security Questions?	1
NAU Username / UserID?	4	SSN?	4
NAU Email?	2	NAU ID / Jacks Card?	6
Student Type, Admit Term/Status, Campus, etc.?	3	Driver's License / State Issued ID / Passport?	5
DOB?	5	Biometric?	0
Address?	2	Other?	4

Criteria: Sound business practices and strong internal controls include the development of policies and procedures designed to ensure consistency in how functions meet corporate objectives. Additionally, as NIST is the IT Security framework of reference used by NAU ISS, such policies and procedures should be linked to NIST standards and / or guidance. The most recent NIST guidance applicable to identity verification or authentication is the NIST Special Publication 800-63-3 Digital Identity Guidelines, which includes the following:

“The classic paradigm for authentication systems identifies three factors as the cornerstones of authentication:

- Something you know (e.g., a password).
- Something you have (e.g., an ID badge or a cryptographic key).
- Something you are (e.g., a fingerprint or other biometric data).”

It then includes guidance in the application of the above based on nature of the evidence in each of the categories that individuals should provide in each situation.

Cause: To date, development of centralized identity verification guidance has not been prioritized.

Effect / Impact: While no recent instances of inappropriate access through failure to properly authenticate have been identified, the lack of consistent verification processes could result in authorized system access and data compromise.

11. Updating applicable policies and procedures and requiring routine review of local administrator account analyses and communications could improve NAU’s mitigation of risks associated with unauthorized use of local administrator accounts.

Solution: Update and implement the Access Management Policy and standards to specify how local administrator accounts on University-owned personal computing equipment may be used and how they should be managed, including:

- Removing local administrator accounts upon completion of support work.
- Training all system administrators and technicians on policy.
- Establishing a periodic review routine to identify and report violations to applicable ITS Directors and conduct follow-up activities to ensure violations are adequately addressed.
- Establishing a monitoring routine.

Audit Results: Improvement Opportunities & Solutions

Responsible Parties:

Suzanne Hanks, Director, Service Desk & Technical Support Services
Michael Zimmer, Director, ISS
Trey McCallie, IAM Team Lead, ISS

**Implementation
Date:**
12/31/2020

DETAILS:

Condition: Local administrator accounts on University-owned personal computers/tablets/etc. are used by ITS support personnel to help address computer performance issues and repairs and handle new software installation needs identified by NAU employees and other individuals using University-owned computers. There is no routine process for analyzing and managing the use of these local administrative accounts and while there is appropriate policy addressing such, compliance appears poor and without periodic analysis and enforcement.

Current use of local administrator accounts does not appear to support related policy requirements as evident per the following:

- ITS acted in response to the request made by this audit by completing a high-level analysis of local administrator account usage in January 2020, noting a high number of existences of inappropriate local administrator accounts.
- Based on this initial analysis, ITS Service Desk & Technical Support Services issued a cease and desist memorandum on February 5, 2020. The memorandum was issued to applicable ITS personnel and instructed removal of all local accounts utilizing two specific, commonly used account names. ISS also implemented a policy to employ a script that automatically and perpetually removes the two accounts on system login. Both actions appear to have been effective in reducing the existence of those accounts:
 - The overall number of Group Administrator accounts in violation decreased (from 235 in January 2020 to 204 in May 2020).
 - The number of individual instances / existences of Group Administrator accounts deemed in violation of the policy decreased by 47% (from 3,249 in January 2020 to 1,721 in May 2020).

While a routine process for analyzing and managing the use of local administrator accounts is not yet in place, the efforts implemented following the January review resulted in a significant decrease of local administrator accounts on desktops and laptops. However, 1,721 local administrator accounts deemed in violation continued to exist as of May.

Criteria: The Appropriate Use of Technology Policy requires system administrators and technicians to maintain data integrity and protect IT resources. Also, per the Device Configuration Standards, Section III, "Access should be via unique ID per individual and all University Community Members must comply with the Appropriate Use of Information Technology Resources policy. And, where possible, limit the use of Administrator accounts for system administration services only." Also, the draft Access Management Standard notes that Privileged Access accounts, which would include local administrator accounts, pose significant cyber risk to NAU:

"Section I. – Standard Access

Audit Results: Improvement Opportunities & Solutions

1.2 Multiple Digital Identities

Some members of the University community may be granted multiple Digital Identities to support their role at the University. These accounts must be associated with the user's NAU User Account and must be deprovisioned upon the University Community Member no longer holding an active affiliation or upon a role change that no longer authorizes the utilization of the provisioned digital identity.

Section II. – Privileged Access

1. Definition and Description

1.1. Privileged Access, often referred to as “administrator”, “admin”, “root”, “service”, or “Privileged” access, exists in all operating systems, databases, and applications. Privileged Access is commonly used for running specific services or processes that typically have elevated privileges that allow for modifications to the operation of an IT Resource, and full access to files, logs, and other user account privilege levels.

1.2. Due to the nature of the high level of access, accounts associated with these rights are targeted by attackers seeking to compromise and use them for unauthorized access. The compromise of a Privileged Access account poses significant risk and harm to the University, including data loss, creation of attacker-controlled accounts, and continued control of IT Resources.”

The Appropriate Use of Information Technology Services Policy requires that System Administrators and Technicians, "maintain the privacy and confidentiality of sensitive information seen or obtained in the normal course of their work, and report suspected violations of the University's IT Resource policies or standards to the appropriate University officials" and that, "granted significant privileges and trust to use their IT Resource authorizations appropriately and only for the intended purposes."

The Device Configuration Management - Device Configuration Standards requires System Administrators and Technicians per Section III Endpoint Configurations Standards to, "Access should be via unique ID per individual and all University Community Members must comply with the Appropriate Use of Information Technology Resources policy....[and]....Where possible, limit the use of Administrator accounts for system administration services only."

Cause: Enforcement of policy and standards and routine monitoring of local administrator accounts was in the process of being more formalized at the time audit fieldwork was completed. While swift action was taken to address the immediate issue, more notable changes should be anticipated as increased monitoring efforts are implemented.

Effect / Impact: Unnecessary, unauthorized, and / or unused local administrator accounts provide easy access points that allow for undetected movement through the network from one device to another until larger system compromise occurs. Multiple unauthorized uses of standard local administrator accounts across numerous endpoint devices exposes the University's systems to substantial risk.

EXHIBIT A – Background Information
(Page 1 of 2)



Figure 1. Identity Lifecycle

Identity and Access Management (IAM) is the process used in business and organizations to grant or deny employees and others authorization to secure systems. Figure 1 reflects the identity lifecycle stages from the relationship beginning (account provisioning) to end (account de-provisioning)⁶.

Although identity and access management are a shared responsibility, NAU's Identity & Access Management team is tasked with administering the University's comprehensive IAM program to help maintain the availability, confidentiality, and integrity of University information. Applying the NIST Cybersecurity Framework, the office provides IAM services including password management, authentication and authorization systems reviews, user lifecycle management, privileged access management, incident response, guidance for complying with IAM controls, oversight of IAM activities, and other related services.

The NAU Information Security Program has an established governance structure to continually monitor and improve upon services, establish measurements of success, and assess the program. The Information Security Committee is part of the University's IT and Data Governance structure that reports to the Chief Information Officer (CIO). This committee is responsible for oversight of the Information Security Program, providing:

- 1) Recommendations to the CIO regarding information security policies and standards; and
- 2) Guidance and support to the Director of Information Security for the implementation and maintenance of the Information Security Program.

Affiliate Accounts

Affiliate accounts are managed by ITS Strategic Planning, Implementation and Education Services (SPIES). As of January 2020, there were 3,594 active affiliate accounts. Affiliation is a general term that can include several potential relationships with NAU, such as identification management (informational) only, formal employment, partnerships with community and / or fraternal organizations, and / or to facilitate collaborative academic work. Individuals or groups who have a legitimate University affiliation, combined with a valid need for privileged access to buildings, email, and networking services, may be granted services based on affiliation types. Affiliation types may be supported by ITS, Human Resources, the President's Office, and / or the Provost's Office, and most typically provide NAU computer access, University email access, and NAU ID access.

⁶ <http://www.blog.itil.org>. (Date Accessed: 7/14/2020)

Northern Arizona University
Access Management
Internal Audit Report
October 2, 2020

EXHIBIT A – Background Information

(Page 2 of 2)

Physical Access

Management of access to University structures containing wiring closets, utility tunnels, data centers, and server rooms is largely decentralized and consists of both manual and electronic processes. Multiple University areas are involved in managing and monitoring building access and security, including Facility Services, ITS Infrastructure & Platform Services, Campus Services & Activities (CSA), and NAU Police Department. The Lenel badge system is used to assign access levels, deactivate and reactivate badges, delete cardholders and badges, and report badge activity by cardholders having either the JacksCard or Legacy badge (a consolidated card used by long-term NAU affiliates only). Physical access to residence halls is controlled and managed using the JacksCard and / or Legacy badge.

Salesforce Logical Access

Salesforce CRM is a hosted application for Call Center and Case Management overseen by ITS Enterprise Information Services. NAU deployed Salesforce campus-wide in 2016 as an effort to build a connected campus, improve student retention, and facilitate student success. The objective of Salesforce is to modernize service and personalize marketing while also engaging and addressing unique needs of University users. ITS leverages the existing electronic PeopleSoft Application Security System (ePASS) hosted in PeopleSoft Human Capital Management (HCM) to help manage and document access to data in Salesforce.

Identity Verification

Identity verification is the process of validating the claimed identity of an individual and is central to a secure and authoritative process for the issuance and use of identity credentials. Identity verification can be accomplished through a variety of processes that establish a history of identity by collecting identity information, such as personal, demographic, and biological data, and validating the accuracy and legitimacy of the information collected by conducting a face-to-face interaction and / or verifying the validity of the source data against personally identifiable information (PII) stored in University databases.

Local Administrator Accounts

Privileged access exists in all operating systems, databases, and applications and is managed by ITS Service Desk & Technical Support Services. Administrator accounts are commonly used for running specific services or processes and typically have elevated privileges to allow for modifications to the operation of an IT resource and full access to files, logs, and other user account privilege levels.

This page intentionally left blank