NORTHERN ARIZONA UNIVERSITY

Internal Audit Department

Shadow IT

(Part 1 of 2)

~~**October 21, 2019**~~
Revised October 24, 2019

Report Number FY 19-07

Distribution:
Audit Committee, Arizona Board of Regents
Internal Audit Review Board
Rita Cheng, President
Steve Burrell, Vice President and Chief Information Officer
Bjorn Flugstad, Vice President, Finance, Institutional Planning and Analysis
Mark Grisham, Director, Policy and Special Projects
Joanne Keene, Executive Vice President and Chief of Staff
Celisa Manly, Director, Information Technology Service Management
Michelle Parker, General Counsel
Albert Sandoval, Director, ITS Business Services
Wendy Swartz, Associate Vice President and Comptroller
Brett West, Director IT Operations
Michael Zimmer, Director, Information Security

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 sub-recipients.

This page intentionally left blank

Northern Arizona University
Shadow IT (Part 1 of 2)
Audit Report
October 24, 2019

Summary

Audit of Shadow Information Technology (IT) is in the Annual Audit Plan for Fiscal Year 2019, as approved by the Audit Committee of the Arizona Board of Regents. This audit supports Northern Arizona University's (NAU / University) strategic goals of Student Success and Access, and Stewardship by helping to ensure that NAU protects University and related NAU community data resources.

Background: Shadow IT is the use of information technology-related hardware, software or services by any member or function of the NAU community without the approval, knowledge and support of NAU Information Technology Services (ITS), and existing outside NAU's selected control framework. NAU IT Security aligns with the National Institute of Standards and Technology (NIST) framework for cybersecurity and risk assessment purposes. Shadow IT is of most concern to NAU when used to manage, store or share sensitive data, or to manage and process business critical transactions.

Shadow IT can include the use of locally installed hardware and / or software as well as third-party applications, including cloud services. Typical uses of applications like word processors and spreadsheets would not typically be considered Shadow IT except when supporting sensitive data and / or business critical transactions. In recent years and across all industries, cloud services represent the most prevalent form of service-oriented Shadow IT.

Ease of adoption, rapid deployment and cost savings can make Shadow IT solutions appear beneficial to users of that information technology. However, without consideration for the related risks, such adoptions may result in negative exposure to the broader NAU community as well as to the individuals using the Shadow IT. The major downside risks of Shadow IT include:

- Security of data stored locally or by third-party vendors may be compromised without NAU's knowledge or ability to address.
- Fines, lawsuits and legal fees may result from failure to comply with data privacy and other regulations or the loss of and failure to report lost confidential or consumer information.
- Lack of knowledge of Shadow IT solutions could cause unnecessary or extended downtime in the areas using Shadow IT and / or loss of time and productivity in other areas of NAU.
- Shadow IT increases the complexity of the overall IT infrastructure by creating instances of IT that are either unknown or require management / oversight outside existing IT operations, thereby increasing the risk associated with business disruption, incident response and overall technology and data protection efforts.
- Unanticipated costs may increase and other complications may arise in relation to services provided by third-party development vendors (e.g., unsecured or lapses in security over cloud services) and / or lack of a robust third-party infrastructure.

In recent years, NAU moved to centralize information technology resources to improve oversight of IT-related risks, improve overall service delivery, and improve its ability to comply with notable regulations, especially those focused on protecting sensitive data, such as the Family Educational Rights and Privacy Act (FERPA) and the Health Insurance Portability and Accountability Act (HIPAA). Centralization does not mean that all IT resources are physically co-located; instead centralization's goal is to organize all IT under the authority of the Chief Information Officer. This effort resulted in development of stronger overall IT governance supported by NAU-wide IT policy, procedure, and practice, including the ability to more readily identify Shadow IT.

Northern Arizona University
Shadow IT (Part 1 of 2)
Audit Report
October 24, 2019

Audit Objectives: The primary objective of the audit was to determine if NAU manages its information technology resources such that technology deployed is centrally approved, managed or known by NAU ITS. We also sought to identify any Shadow IT that may currently exist, although more focused work in that regard will be pursued in part 2 of 2 of the Shadow IT audit effort.

Scope: Due to the nature of timing of our audit efforts and major initiatives at NAU that impacted our ability to pursue certain analyses and tests, we divided the audit into two parts: this report addresses the audit scope for part 1 of 2, which included*:*

- Review of all policies, procedures and practices governing the management of information technology as it may relate to NAU's oversight of information technology and the related management of electronically stored data.
- Review of those policies, procedures and practices for applicable controls and best practices supporting NAU's oversight of information technology in a manner that minimizes Shadow IT use.

We conducted such analyses, tests and other procedures as we deemed necessary to address the audit objectives.

Our scope is limited by the availability of trained IT audit resources. As such, we did not attempt system analysis, scans or other tests that require specific technical knowledge and skills.

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

- Analyzed alignment of the NIST control framework to applicable ITS and other NAU policies, procedures and practices related to the management of IT resources.
- Analyzed NAU IT procurement practices to ensure those practices could identify potential purchases with resulting Shadow IT implications or implementation.
- Analyzed the application of IT-specific restrictions and practices as applied that could prevent and / or detect the use of Shadow IT.
- Applied procedures designed to identify any unknown Shadow IT currently in use, including identifying all critical systems in use as we completed the other audits included in our ABOR approved Fiscal Year 2019 Internal Audit Plan.

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		
0	1	4

NAU has implemented IT policies, procedures, protocols, standards and practices (see Exhibit A) that align with the NIST framework including "Appropriate Use of Information Technology Resources," "Device Configuration Management" and computer procurement related policies and standards. Formal training is also required as it relates specifically to IT security matters, including appropriate use and data protection. These activities support positive IT governance including appropriate oversight and management of <u>all</u> NAU IT resources, which thereby minimizes risk associated with Shadow IT.

Based on the limited tests applied in Audit Part 1 of 2, we identified no obvious instances of Shadow IT. Expanding NAU's network scanning and analyses could result in more timely and complete prevention and detection of Shadow IT.

Observations: NAU's IT centralization effort created an environment that allows for improved control over NAU information technology in terms of what can be used, who can use it, how it is used and how related data is managed. However, such a structure does not guarantee Shadow IT has been eliminated or that local information technology implementations are not or will not be permitted. Tolerance for IT that is not centrally managed by NAU ITS is still being determined as it depends on various factors including:

- the nature and purpose of any identified IT system or service,
- the nature of data at risk,
- the intentions of the individuals or functions using the IT,
- the robustness of locally implemented controls over that IT and related data, and
- net cost or value to NAU of allowing the implementation.

Additionally, the determination that a given use of IT would be considered Shadow IT includes consideration for its relative risk to NAU relative to:

- Use or storage of Sensitive Data on system(s) not recognized or sanctioned by the CIO;
- An implementation of IT that, by design, obfuscates the presence of a device(s) / data from institutional authorities;
- An implementation of IT that, by design, obfuscates the purpose for which it is intended; and,
- An unnecessary replication of data / logic that incurs substantial expense or use of resources.

In this regard, part 2 of the audit effort in conjunction with NAU IT Security department data surveys and analyses will help guide related decisions and any need for improvement to existing policies, procedures, standards and practices. Such will be reflected in the report on Shadow IT Audit, Part 2, to be completed in fiscal year 2020.

This initial audit effort resulted in robust conversations and considerations around the Shadow IT concept. In this regard, management has implemented or is implementing the following improvements that should result in the continued maturation of its efforts to manage NAU IT risk, including risk associated with Shadow IT:

- Centralizing its formal information technology inventories. NAU ITS currently maintains six different inventories including services or product offerings; academic and research software; network, services and telecommunications; custom applications; desktops, laptops and peripherals; and other software.
- Implementing IT policy, procedure, practice and standards relative to NIST guidance with formal review cycles to ensure such direction and guidance remains current and effective. Current related policies, procedures and standards are listed in Exhibit A.
- Applying centralized, strategic IT project management services, including procedures for proposing or requesting IT projects, and project prioritization and selection processes.
- Providing IT security training supporting established policy, procedures, practices and standards.
- Updating its Device Configuration Management Policy to apply to all NAU IT systems, as recommended by the Arizona Office of the Auditor General in its Information Technology Security performance audit report issued in June 2018.
- Working together with Internal Audit on surveys, networks scans, and other analyses to help identify any current instances of Shadow IT.

The control standards considered, related control environment assessment and any related improvement opportunities (IO) 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.
Reliability and Integrity of Financial and Operational Information: Controls Not Applicable			
Safeguarding of Assets & Compliance with Laws and Regulations:			
• Policies and procedures are designed and implemented to ensure only authorized information technology is in use.			
• Information technology assets are formally inventoried to ensure all authorized information technology is identified and available for comparison.			
• System analysis and scanning tools are deployed to ensure only authorized access and use of NAU information technology and as a means to prevent and detect the unauthorized use of Shadow IT.		1	5
• IT procurements (including hardware, software and services) require advance assessment, review and approval by ITS.			
Effectiveness and Efficiency of Operations:			
• NAU faculty and staff are made aware of the risks associated with using unauthorized information technology and their related responsibilities for protecting University information and IT Resources.			

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

We appreciate the assistance provided by the staff and management of Information Technology Services and the Policy Management Office.

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. The expansion of network analyses could reduce the risks associated with the implementation and use of Shadow IT.

Solution: As resources permit, identify existing and available tools and create an approach for routine or periodic scanning for unauthorized systems and / or data usage. Analyze existing and available scanning and analysis options and develop a plan for routine or periodic scanning and analysis. Additionally, apply user restrictions where possible to prevent, within the confines of "academic freedom", intentional and unintentional access to web sites and other IT resources that could cause harm to NAU.

Responsible Parties:

Brett West,
Interim Director ITS Infrastructure & Platform Service
Michael Zimmer, Director IT Security

Implementation Date:

January 1, 2020

DETAILS:

Condition: NAU ITS has implemented the following technical procedures that help to minimize the likelihood of Shadow IT:

- Physical connections to the NAU network require device registration which requires authentication, authorization and accounting (AAA).
- The NAU wireless guest network is open to the public but is segmented from the rest of the NAU network. Wireless network otherwise requires AAA or device registration, which also requires AAA.
- ITS responds to detections of malicious or suspicious software, which in almost all cases are unauthorized. These incidents are handled with the typical response steps: prepare, identify, contain, eradicate, and recover.

While ITS uses certain network scanning and other network analysis tools, they are not currently deployed as a deterrent and detection process for Shadow IT.

Criteria: Best practices as identified in various IT frameworks like NIST (National Institute of Standards and Technology), COBIT (Control Objectives for Information and Related Technologies) and ITIL (Information Technology Infrastructure Library) identify the need to proactively address Shadow IT.

Cause: Resource availability and competing priorities.

Effect / Impact: Inability to deter or detect unauthorized systems / data use.

EXHIBIT A
List of NAU Policies and Procedures Supporting Control Over Shadow IT
(Policy and Procedure Versions as of September 5, 2019)

NAU Policy & Procedure	Shadow IT Risks Addressed
1. Comptroller: Prohibited Transactions	Prohibits the purchase of IT related services including: Internet Service Charges and Software (without prior ITS approval).
2. Equity & Access Office: ICT Use and Purchase Procedures	Requires all Information and Communications Technologies (ICT) pursued to be reviewed prior to purchase to ensure compliance with Section 504 of the Rehabilitation Act of 1973 by being appropriately accessible to individuals with disabilities.
3. Human Resources: Use of University Property (HR Policy 5.14)	Provides that, "all university property is to be used strictly for University business, and allows no expectation of privacy…." including, "All desks, files, lockers, vehicles, computers (including the campus electronic mail system and network access), telephones, other office equipment, and other university-owned property…" and further notes that, "All property….belonging to the university for which the university is responsible, is to be used solely for university purposes…" and, "Those using computer resources and networks belonging to Northern Arizona University must act in a responsible manner, in compliance with law and policies, and in accordance with the ITS Appropriate Use of Information Technology Resources Policy and related Standards."
4. ITS: Access Management Policy (Draft as of 9/5/2019)	Establishes the collective University Community responsibility for protecting access to University information and IT Resources, minimum applicable standards for access, responsibility for reporting potential inappropriate access and requirement for University Community members to know the policies and related standards.
5. ITS: Appropriate Use of Information Technology Resources Policy and related Standards	Addresses the appropriate use of NAU technology used at the University. Establishes the parameters / standards for appropriate use of University IT Resources with a focus on six guiding principles: 1. Use only the IT Resources authorized to use; 2. Only use the University's IT Resources for authorized purposes; 3. Abide by all applicable laws, regulations, policies and contractual / licensing agreements; 4. Take reasonable care to protect the integrity of the University's IT Resources; 5. Respect the privacy / personal rights of others; and, 6. Do no harm. The policy requires authorized users to, "…affirm their knowledge of this policy and its associated standards of appropriate use…" and identifies "Use of the University's IT Resources is a privilege granted to Authorized Users in furtherance of their educational opportunities or professional duties and responsibilities. The CIO may temporarily suspend or permanently revoke an individual's access to the University's IT Resources if necessary to protect or maintain the integrity or security of the University's IT systems or data." The related Standards identify the restricted use of University IT Resources to those authorized and supportive of the NAU mission, set parameters for the personal use thereof, and identify various disciplinary situations. In this regard the policy provides for disciplinary action up to and including access revocation and employment termination.

EXHIBIT A **List of NAU Policies and Procedures Supporting Control Over Shadow IT** **(Policy and Procedure Versions as of September 5, 2019)**	
NAU Policy & Procedure	**Shadow IT Risks Addressed**
6. ITS: Computer Purchasing Policy / Procedure	Establishes a centralized computer hardware standardization and purchasing program for Desktops, Laptops, Tablets, and Workstations purchased with University funds and indicates that all NAU employees who use computer equipment should know the policy. Addresses the process for reviewing or changing standard configurations; the process to request computer purchase exceptions; and the purchasing procedures required for computer purchases including review by an ITS Computer Purchasing Manager and ITS Computer Hardware Committee. The policy specifically states that ITS "will not support non-compliant or unapproved computers."
7. ITS: Data Classification and Handling Policy and related Protocols	Requires "…all data and information systems and devices owned by or under the University's control…" to be classified according to the four-level classification protocol.
8. ITS: Device Configuration Management Policy and related Standards	"This policy establishes baseline controls and standards for the management and maintenance of the University's Information Technology ("IT") Resources… All units and University Community Members are responsible for classifying all data within their care and implementing appropriate device configuration standards to protect the data." The related Standards apply to, "…three separate categories of devices, which are: a) University servers; b) University desktops, laptops, tablets, and all other mobile computing devices (collectively referred to as "Endpoints"), and c) all types of non-University computing devices (collectively referred to as "Personal Devices")." • Requires, "…all Personal Devices used to access Sensitive Information must adhere to the Device Configuration Standards…", which "…outlines the appropriate uses, device settings, procedures, responsibilities, and the conditions, risks, and liabilities associated with using Personal Devices to fulfill professional obligations such as accessing or working with Sensitive Information." • Requires, "System Administrators and Technicians configuring, installing, or deploying new University IT Resources must maintain secure configuration baselines for servers and Endpoints." With additional details regarding minimums and required documentation and reviews. • States that, "These standards shall apply to <u>all data processing or computing devices capable of connecting to or interacting with the University's IT networks</u> and shall reflect and promote data handling best practices and compliance with all applicable laws, regulations, policies, and contractual or licensing requirements." With noted required minimum standards. • Provides the requirements associated with using a personal device to access NAU IT Resources. • Provides for disciplinary action up to and including access revocation and employment termination.
9. ITS: Information Security Awareness Training Policy	Establishes required IT security training for all authorized users of NAU IT.

EXHIBIT A
List of NAU Policies and Procedures Supporting Control Over Shadow IT
(Policy and Procedure Versions as of September 5, 2019)

NAU Policy & Procedure	Shadow IT Risks Addressed
10. ITS: Information Security Policy and related Standards	Establishes an Information Security Program and the requirement for compliance with it, along with disciplinary measures up to and including termination for non-compliance. Places responsibility on each "senior executive" to ensure implementation of related IT security practices in their area of responsibility. Requires all University Community members to report any lapses, breaches, etc. Establishes the requirement for "…providing all training that may be necessary or prudent." The related standards address: Auditing, Logging, and Monitoring; Data Backup and Disaster Recovery; Enterprise System Change Management; Information Technology Risk Assessment; Secure Data Center Physical Security; Software Patch Management; and, Vulnerability Management and Scanning.
11. ITS: Information Technology Incident Management Policy and related Procedure	Encourages "University Community Members who use the University's IT Resources…. to immediately report suspected IT Incidents or Major IT Incidents to Information Technology Services."
12. ITS: Project Management	Provides a project management oversight and prioritization process to ensure focus on resourced IT priorities.
13. NAU: Conditions of Faculty Service	Applies to all NAU Faculty including chairs, deans, vice provosts, provost and faculty senators. It notes that, "In accordance with ABOR Policy 6-201, the 'duties of a faculty member shall consist of those responsibilities assigned by the president of the university or an appropriate administrator, such as a vice president, dean, director or department head / chair. Teaching assignments, schedules and other instructional responsibilities shall be carried out under the direction of the president. Duties and responsibilities shall be related to the expertise and competence of the faculty members and may include sponsored or unsponsored research projects, service activities, or administrative functions.'"
14. Purchasing Department: Conflict of Interest	Requires "All NAU employees" to "comply with the State of Arizona conflict of interest laws."
15. Purchasing Department: Purchase Orders & Requisitions	Prohibits the purchase of computers and software using a departmental purchase requisition.
16. Purchasing Department: Purchasing Cards	Prohibits the purchase of computers, software or related services using an NAU Purchasing Card.