Executive Summary: A Review of the University of Arizona's Information Technology Services

The ad-hoc General Faculty Committee on Information Technology has written a sixty page factual review of the Office of the Chief Information Officer (CIO) and Central University Information Technology Services (UITS) strategy, security, centralization, cloud, research computing, and data management . We summarize our preliminary findings below.

§1 Recent History & UITS Leadership

The University of Arizona CIO Division has over 350 employees and an annual operating budget of approximately $77.6M (million)[1]. The Campus IT had ~320 employees, who are now part of UITS. The total IT (Central + Campus) expenditure for the UArizona in Fiscal Year 2022 (latest available data) was $140.98M.

A recent statewide security audit (2018, 2022) and the late 2023 announcement of a financial crisis at UArizona resulted in a Financial Action Plan which mandates centralization of all IT at UArizona[2]. IT centralization has been a goal of the administration for several years and it is now ostensibly achieved through the 2024 mandate.

The Chief Information Officer (CIO) Barry Brummund serves concurrently as the Vice President of University Integrated Planning Office[3]. At this critical time, he has delegated responsibility of managing UITS to his deputy Lanita Collette but still retains decision making authority and therefore is responsible and accountable for Office of the CIO actions.

§2 Security

The June 2018 "Arizona's Universities - Information Technology Security" Performance Audit[4] found University of Arizona was deficient in 23 recommended areas. A 48-month follow-up report published in August 2022 (see report §2.1) found only 5 recommendations had been implemented, 12 had been partially implemented, and 6 were still not implemented[5]. The absence of detailed explanations for the audit's recommendations indicates a lack of transparent planning and accountability, which could hinder the effective mitigation of IT security risks.

UITS has demonstrated a commitment to enhancing cybersecurity measures through the implementation of multi-layered security strategies, such as security awareness training, robust access control, and incident response planning. However, the 48-month follow-up audit revealed significant shortcomings in the university's cybersecurity posture, with only a fraction of the recommendations fully implemented and several critical areas still lacking progress. This suggests a gap in the execution of comprehensive security measures and a potential vulnerability to cyberthreats.

[1] https://web.archive.org/web/20231210052341/https://it.arizona.edu/about-us/cio-division
[2] https://it.arizona.edu/it-centralization/centralizing-information-technology-services
[3] https://universitysecretary.arizona.edu/university-planning
[4] https://www.azauditor.gov/sites/default/files/2023-11/18-104_Report.pdf
[5] https://www.azauditor.gov/sites/default/files/2023-11/18-104_48-Mth_Followup.pdf

In March 2023, the [former] Vice President of Research (Betsy Cantwell) and CIO (Brummund) announced the Arizona Secure IT Services (ASITS) initiative[6] in response to the follow-up audit. ASITS quickly became unpopular with academic departments and research units for numerous reasons (see report §2.2 and §3.5) related to its costs and perceived loss of supervisory control. IT centralization will provide the Office of the CIO with the ability to initiate control and implement all of ASITS under its new umbrella.

§3 Centralization

Approximately 625 employees and $400M in research funding are directly affected by the IT centralization. Details about the re-organization and reporting structures are still in development and have not been announced by the Office of the CIO.

The Office of the CIO executed the IT centralization plan without consultation from the Colleges, Faculty Senate, the Deans, or the Vice President for Research, stakeholders, or its institutional partners. This set a dangerous precedent and is a unique event across R1 institutions with large IT departments. Rapid IT centralization mandates now endanger federal research projects and agreements (see report §3.4).

The abrupt March 2024 IT centralization approach has raised concerns about diminishing domain-specific knowledge, loss of proximal IT support, and potential disruptions to the educational and research missions. This could lead to a reduction in the effectiveness of departmental IT services and a loss of tailored support that directly addresses the unique needs of stakeholders.

§4 Cloud Services

The migration to commercial cloud services, particularly Amazon Web Services (AWS), offers the University of Arizona the opportunity to modernize its IT infrastructure, achieving scalability, flexibility, and access to advanced technologies and services. Nevertheless, the transition to cloud computing introduces challenges such as potential vendor lock-in, unexpected cost variances (especially related to data egress and storage), and the complexities of managing cloud-based services. These risks necessitate careful planning and mitigation strategies to prevent dependency on a single provider and ensure that cloud services remain cost-effective and aligned with the university's diverse needs.

§5 Research Computing and Data Management

UITS Research Computing provides the faculty and staff with an equivalent value of $16.5M per year relative to similar resources on AWS[7]. In 2021 and 2022 campus high-performance computing (HPC) resources supported

[6] https://research.arizona.edu/announcements/secure-it-services-university-research-activities
[7] https://it.arizona.edu/news/high-performance-computing-research

$395M and $382M in sponsored research expenditures, respectively[8]. Moving HPC onto a commercial cloud provider could result in UArizona HPC costs increasing by an order of magnitude.

The University of Arizona's dedication to supporting HPC and data storage for research demonstrates a robust infrastructure capable of supporting a wide range of scientific inquiries. However, the reallocation of funds from HPC hardware refresh to enterprise software licenses without consulting the HPC user community has led to frustration and confusion. The currently limited availability of graphic processing units (GPU) resources necessary for Artificial Intelligence (AI) applications places constraints on the university's capacity to conduct top-tier AI research and to train large language models used for generative AI[9].

§6 Recommendations

Encouraging the Office of the CIO to engage with faculty and researchers to develop new committees around IT decision making could strengthen UITS leadership and improve morale across campus IT units. Other R1 universities which have Information Technology Advisory Councils (ITAC)[10] responsible for guiding IT decisions through their offices of IT with shared governance could be used as templates (see §6.3.3).

We encourage a hybrid approach to the centralization of IT security. A hybrid approach includes: high level security policies and protocols which are governed from Central IT, while allowing individual departments and research units the autonomy to implement additional specific security measures tailored to their needs.

UITS now has the potential to significantly enhance services and opportunities for the University of Arizona community through strategic centralization, cloud migration, and dedicated support for research computing and data storage. We also reemphasize that the adoption of cloud computing and commercial cloud providers is not a *zero-sum* or *all-or-nothing* decision. Hybrid cloud, on-premises, and HPC solutions for research computing are the recommended framework.

IT centralization and cloud services has been stated as being aimed at improving security compliance, operational efficiency, and financial management. Recent annual reports from UITS (see §3.1) have emphasized UArizona IT's already impressive financial efficiency and cost-saving in operations relative to other peer institutions, this undermines the justifications for centralization as a means of improving operational and financial efficiency.

[8] https://www.annualreport.it.arizona.edu/sites/default/files/2022-04/UArizona_IT_AnnualReport_FY2021_0.pdf
[9] https://developers.redhat.com/articles/2022/11/21/why-gpus-are-essential-computing
[10] https://itac.duke.edu/, https://www.colorado.edu/information-technology/it-governance, https://it.tamu.edu/about/it-governance/index.php

Draft Report: A review of The University of Arizona's Information Technology Services strategy, security, centralization, cloud, research, and data management

Table of Contents

§1 Introduction

This draft report serves as a factual review of the University of Arizona (UArizona) Information Technology (IT) Services (UITS) unit and its recent strategy to meet the requirements of compliance as a function of both the 2018 statewide IT security audit (§2) and the 2024 Arizona Board of Regents (ABOR) mandated centralization of UITS (§3). We present details about the migration of IT services onto a commercial cloud provider (§4), the role of research computing and data management (§5), recommendations to consider (§6), and provide supporting materials (§7).

§1.1 Purpose

The purpose of this report is to inform the Faculty Senate on the current UArizona IT landscape, the role of UITS at UArizona, and the impact of IT on services, security, networking, and research computing as they pertain to the university's mission of teaching, research and innovation.

The goal of this ad-hoc committee is to foster productive conversations amongst stakeholders which value co-production, equity, and inclusion. Critical in nature, this report is also intended as a check on executive actions which have happened unilaterally without the input of UArizona stakeholders who rely on critical IT for their existence.

§1.2 Committee Members

This ad-hoc General Faculty Committee on Information Technology was formed at the behest of the Faculty Senate President Leila Hudson in late December 2023 and early January 2024. The members of the committee were selected for their domain expertise in data science, research computing, cyberinfrastructure, security management, networking, and experience working with the Office of the Chief Information Officer (CIO), UITS infrastructure and its staff.

Committee Member Names, Titles, Roles, and Departmental Unit:

Tyson L. Swetnam PhD (Committee Chair)[1], Associate Research Professor of Geoinformatics, Director of Open Science, Institute for Computation and Data-enabled Insight (ICDI), Research Innovation & Impact (RII)

Ali Bilgin PhD, Associate Professor of Biomedical Engineering, Electrical and Computer Engineering, and Medical Imaging

[1] Contact email: tswetnam@arizona.edu

Chi-Kwan Chan PhD, Associate Astronomer/Professor, Steward Observatory

Kristina Currans PhD, Associate Professor of Urban Planning, College of Architecture, Planning and Landscape Architecture

Leo Enfield, Information Technology Manager, Electrical and Computer Engineering, College of Engineering

Robert K. Lanza Information Technology Support Analyst, Principal Building Manager, Norton School of Human Ecology

Brian LeRoy PhD, Professor of Physics, Associate Department Head Physics

John D. Moeller, Director, Academic and Research Technologies Group, Eller College of Management

Kristina Riemer PhD, Director of Communications and Cyber Technologies (CCT) Data Science Team, Arizona Experiment Station

Henry Werchan, Assistant Professor of Practice, College of Applied Science and Technology (CAST)

§1.3 Scope

The charge given to the ad-hoc General Faculty Committee on Information Technology is to generate one or more white papers in the Spring 2024 (this draft report), and again in Fall 2024.

We were tasked with "*assessing the IT landscape especially in light of research and teaching infrastructure needs, the crisis in staffing, the findings of the recent state audit and ABOR mandate, and recommendations about centralization, storage, and meeting the needs of a premier research institution,*" by the Faculty Senate President.

Our endeavor is to present a balanced perspective of IT, the Office of the CIO, and UITS which includes the opportunities and benefits of current strategy as well as potential risks and pitfalls. For every identified risk and pitfall we also suggest alternative approaches and mitigations where appropriate.

The lens through which we have chosen to present our findings are in relation to the primary UArizona stakeholder groups who are fundamental to the existence, purpose, functionality, and operation of the university's IT for academic purposes and research.

The four technical IT sections (§) in this initial draft report are as follows:

§2 – outcomes of the 2018 Security Audit and its 48-month follow up report,

§3 – the 2024 ABOR mandated March 4th UITS centralization effort,

§4 – the adoption of a commercial cloud provider for core services,

§5 – Research Computing & Data Management

Early conclusions and preliminary recommendations are presented last in §6. Supplemental information are given in §7.

§1.3.1 Traditional Stakeholders

We identified the following traditional (core) university stakeholder groups of the UITS system as:

- **Students** – are the primary consumers of IT and UITS provided infrastructure. Students need:
    - Reliable WiFi
    - Account Management
    - Access to software for their coursework
    - A seamless course registration system
    - An online learning platform to attend online-classes
    - Access to materials for all classes including lecture material, readings and e-textbooks

- **Faculty** – are the second largest consumers of IT and UITS provided infrastructure. Faculty use IT for:
    - Teaching
        - Learning management systems
        - Classroom technology
        - Software licensing and installation
        - Curriculum delivery
    - Research
        - Computing
        - Data storage
        - Software licensing and installation
    - Administrative tasks
        - Payroll / Time approval
        - Annual reviews (vitae)
        - Professional development

- **Academic Staff**: includes department chairs, deans, and other academic leaders. Academic staff shape technology decisions around:
    - Research enablement
    - Academic program support
    - Data management
    - Data storage

- **Administrative Staff**: includes registrars, admissions, financial aid, parking and transportation, and human resources. Admin staff rely upon IT for:
    - Student records management
    - Financial systems
    - Human resource platforms
    - Core operations

- **Research Staff**: includes academic units and research staff. Researchers are now working with large "big" data on:
    - High-Performance Computing (HPC)
    - High-Throughput Computing (HTC)
    - Cloud Computing
    - Software Development
    - Data Management
    - Data Storage
    - Software as a Service (SaaS)
    - Infrastructure as Code (IaC)
    - Project Management

- **Libraries:** are curators of information and data. This includes the librarians, who manage:
    - Public and protected data repositories
    - Scholarly and Institutional services
    - Geographic Information Systems

- **UITS (Central)**: The backbone. Central UITS manages the:
    - Physical infrastructure:
        - Building space
            - Electricity
            - Cooling/Water
            - Space
        - Computing hardware
        - Fiber networks (ethernet), Internet2 (Sun Corridor)

        - Wired Network Registration (ports / switches)
        - Phone Lines
        - WiFi
        - Computer labs,
        - Classrooms (projectors, PCs)
    - Virtual infrastructure
        - Phone lines
        - Authentication
        - Email
        - Virtual private networks
        - Software licensing
        - Help desk support
        - Cybersecurity
    - Research computing
        - HPC system administration
        - HTC system administration
        - On-Premises cloud computing
        - Commercial cloud computing providers
    - Scientific Equipment
        - Genetic sequencers
        - Mass spectronomy & gas analyzers
        - Medical devices
        - Optical devices
        - Telescopes & associated infrastructure
        - Eddy covariance towers and weather stations

- **Upper Administration:** includes the President, Provost, Senior Vice Presidents, and their support teams. Upper administration establishes strategic direction and budgets for IT, aligning IT decisions with grand challenges and strategic initiatives.

§1.3.2 Research Stakeholders

- **Extramural Research**: research awards (agreements, grants, contracts, fellowships, scholarships) in academic departments, Centers and Institutes, Cooperative Extension, Experiment Stations, AZGS, and RII is the life blood of our R1 institutional platform. IT infrastructure needs for UArizona research projects are bespoke, highly heterogeneous, and require their own IT staffing. These projects range literally from Astronomy to Zoology.

- **Cooperative Extension & Agricultural Experiment Stations**: the Cyber Experiment Station[2] within the College of Agriculture Life and Environmental Sciences (CALES) and the Arizona Experiment Station support many geographically isolated units across the state facilitating the delivery of educational programs, resources, and knowledge into rural communities via a centralized IT program across Cooperative Extension offices and Experimental Stations in Arizona and New Mexico[3].

- **Astronomical Observatories & Space-Missions**: Steward Observatory and the Department of Astronomy[4], together with the sister units Lunar and Planetary Laboratory (LPL) and the Department of Planetary Sciences[5], have been ranked number one in the country in the US National Science Foundation (NSF) HERD rankings (research dollars expended, all sources) for 35 straight years[6]. In recent times (last five years) they have averaged over $120M of expenditures each year and have an annual economic impact on Arizona of $560M per year. Over 90% of these expenditures are from extramural (i.e. external to UArizona) sources. Steward Observatory, LPL and NSF's National Optical-Infrared Astronomy Research Laboratory (NOIRLab)[7] operate multiple space missions and many telescopes around the world. Astronomy projects at UArizona are funded by an array of federal agencies, including the National Air and Space Administration (NASA), NSF, Department of Defence (DOD), and Department of Energy (DOE).

- **Arizona Geological Survey**: The Arizona Geological Survey (AZGS)[8] is nearly as old as the UArizona, having been founded in 1887. The AZGS is hosted on the UArizona campus and manages an IT infrastructure for geoinformatic analyses and data management. AZGS partners with dozens of state and federal agencies, professional societies, private sector organizations, and other universities.

- **Health Sciences**: UArizona Health Sciences[9] rely upon a wide range of IT enabled equipment which generate sensitive and private patient medical records and data (i.e., HIPAA requirements). The Medical College, School of Pharmacy, and Zuckerman College of Public Health[10] have special needs around data security and privacy, and the training of its users, which their unit IT provides.

§1.4 Historical Contexts

---

[2] https://cct.arizona.edu/

[3] https://uagis.maps.arcgis.com/apps/Styler/index.html?appid=1627d784ec2147a18ff51578a9dc83cd

[4] https://www.as.arizona.edu/

[5] https://catalina.lpl.arizona.edu/, https://catalina.lpl.arizona.edu/telescopes , https://kpno.noirlab.edu/

[6] https://news.arizona.edu/story/nsf-uarizona-again-ranks-among-top-20-public-research-universities-no-1-astronomy-and

[7] https://noirlab.edu/public/

[8] https://azgs.arizona.edu/

[9] https://healthsciences.arizona.edu/search/node?keys=Information%20Technology

[10] https://publichealth.arizona.edu/oit

The UITS as a Departmental unit was first announced in November of 2007[11]. UITS was born out of the centralization of the Office of Student Computing (OSCR), Learning Technologies Center (LTC), and the units formerly known as the Center for Computing & Information Technology (CCIT) – Network Technology Solutions, Computing Infrastructure Services, Administrative Computing & Data Services, and Administration & Financial Management.

In 2007, the new UITS fulfilled the IT needs of that era: managing university owned desktop and laptop computing, and building out internet connectivity and WiFi around campus. At that time, UITS provided active support for: Accounts & Passwords, Network & Telephone Services, Security & Privacy, Learning Technologies, Email, Computing Services, Web Services, and Student Computing Resources.

Over the following years, UITS has grown to approximately 300 staff and its offerings include Cloud Computing and data storage, and modern productivity software.

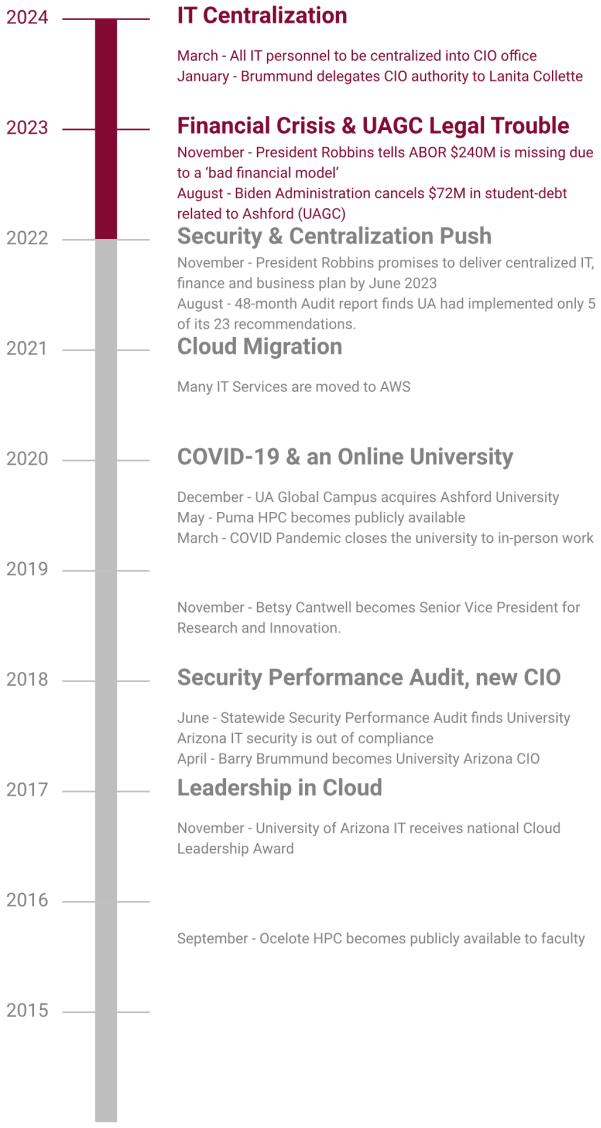


Figure 1: Timeline of recent and relevant events and history around UITS

Across the Academic Colleges and Schools, there are decentralized IT facilities for astronomy, medicine, facilities management, optics, chemistry, bioinformatics, geoinformatics, cyberinfrastructure, engineering, health, and agriculture. Other external IT units include IT units at various research institutes and centers, Arizona Cooperative Extension, Arizona Experiment Station, and Arizona Geological Survey sites across Arizona and New Mexico which maintain their distributed IT in coordination with UITS.

§1.4.1 Recent Events relative to Current Events

[11] https://web.archive.org/web/20071231123121/http://uits.arizona.edu/index.php?id=message

We begin the relevant timeline 11 years ago and continue to the present day:

- The first cloud migrations within UITS began in 2013, culminating in a leadership in cloud award in November 2017[12].

- Mr. Barry Brummund became the CIO of UArizona in April of 2018. In June of 2018 the first Security Performance Audit was released.

- In November of 2019, Betsy Cantwell became the Senior Vice President for Research and Innovation.

- In early 2020 the COVID-19 pandemic greatly impacted how we conduct our teaching and research at the university. In March 2020, staff and students were sent home and we began a two year remote-work experiment which still continues in part today. In May 2020, the new HPC Puma was made available for the first time. In December of 2020, UArizona acquired Ashford University and rebranded it as Arizona Global Campus.

- The full transition of IT services onto cloud continued through 2021.

- In August 2022 a 48-month follow up found the Security audit was still mostly not implemented (see §2). In November 2022, President Robbins made a promise to centralize IT by June 2023.

- In November 2023, CFO Lisa Rulney and President Robbins presented ABOR an unexpected budget shortfall in the range of $171 million, a financial crisis was declared.[13]

- In January 2024, Brummund delegated the role of CIO to his Deputy CIO, Lanita Collette, who is Chief Information Security Officer (CISO). Collette now the [interim] acting CIO[14] was immediately tasked with centralizing UITS[15] and to present her plan to President Robbins in two weeks time.

- On February 14th, 2024 emails were sent to all IT staff that they would be centralized into UITS by March 4th (a three week notice).

§1.4.2 Current and Past UITS Programs

[12] https://it.arizona.edu/news/ua-wins-cloud-leadership-awards, https://www.annualreport.it.arizona.edu/2018-cloud-services

[13] https://www.arizona.edu/financial-updates, https://www.arizona.edu/financial-updates/financial-situation-background

[14] https://it.arizona.edu/person/lanita-collette

[15] https://arizona.zoom.us/rec/play/kXZKWtjT7_GXm8ZRZKxqtcEfhTwLLPm906KvYnEKfabPfWqtxfxfiCWf2U3IjeuD7kXL5MbokynWeyER.IlDYOBhcu4rDtyd9

Arizona Secure IT Services (ASITS)[16] (§2.2) is a comprehensive effort dedicated to reshaping and strengthening IT operations, security, and services across the University of Arizona.

- Identity and Access Management
- Secure Network
- Technology Lifecycle Care (TLC)

Other infrastructure projects include:

- Campus Cloud Infrastructure
    - Managed Cloud Services
- Service Now IT Service Management
- Wired Network Registration

The Research Computing Governance Committee (RCGC)[17] guided the development of central research computing resources at UA and determined how to best serve the needs of researchers across campus. It included:

- Subcommittee on Data Management and Curation[18]
- High Performance Computing [2019 Refresh][19]
- High Performance Computing Policies[20]

RCGC has been less active in recent years, but may see a resurgence in 2025 around the new HPC refresh.

§1.5 UITS Leadership

Our [presumed] UITS Leadership Organizational Chart after March 4th is presented below (Fig. 2). Recent UArizona organizational charts are available with UAccess login credentials here: https://it.arizona.edu/about-us/cio-division. The Office of the CIO organizational staff charts have not yet been updated to reflect the March 4th centralization.

The Chief Information Officer (CIO) and leader of UITS is Barry Brummund[21], who reports to Senior Vice President and Chief of Staff Jon Dudas. Dudas reports to President Robert Robbins. Brummund serves concurrently as the CIO and as the Vice President of University Integrated Planning Office[22] (Fig. 2). Brummund has also previously served as Co-Chair of the Strategic Planning and Budget Advisory Committee.

[16] https://it.arizona.edu/asits/asits-home
[17] https://rcgc.arizona.edu/
[18] https://rcgc.arizona.edu/datamgmt-curation
[19] https://rcgc.arizona.edu/hpc-2019
[20] https://rcgc.arizona.edu/hpc-policies
[21] https://it.arizona.edu/person/barry-brummund
[22] https://universitysecretary.arizona.edu/university-planning

As the Vice President of University Integrated Planning Office, Brummund supports the President and University Senior Leadership "with data-informed research, analysis, and modeling in three key areas:

- ABOR and Tri-University Initiatives
- University Strategic Goals and Metrics
- External Multi-Year and Future Opportunity Strategy and Planning"

Lanita Collette[23] is currently CISO and acting CIO until June 30th, 2024. Collette has been tasked with designing and executing the UITS Centralization effort, but still reports directly to Brummund. The Office of the CIO Organizational Chart shows Collette with 12 direct reports, in Fig. 2 only the senior leadership positions are shown. The other direct reports for Collette include Architect Managers, Communications, Operations, and Network personnel. The core leadership of UITS who directly report to interim CIO Collette: Ravneet Chadha[24] Chief Data Officer (CDO) and Business Intelligence Manager, Maysoon Eshelman[25] Executive Director of Campus IT Partnerships, Susan Legg[26] Executive Director of IT, Michael Medina[27] Executive Director of Support Services, Darcy Van Patten[28] Chief Technology Officer (CTO), Jeremy Frumkin[29] Executive Director of Research Technology, and Chris Wolf[30] Senior Director of Finance & Administration (Fig. 2). Presumably, this is also the team who is advising acting CIO Collette on UITS centralization decisions.

[23] https://it.arizona.edu/person/lanita-collette
[24] https://provost.arizona.edu/person/ravneet-chadha
[25] https://it.arizona.edu/person/maysoon-eshelman
[26] https://it.arizona.edu/person/susan-legg
[27] https://it.arizona.edu/person/michael-medina
[28] https://it.arizona.edu/person/darcy-van-patten
[29] https://it.arizona.edu/person/jeremy-frumkin
[30] https://it.arizona.edu/person/chris-wolf

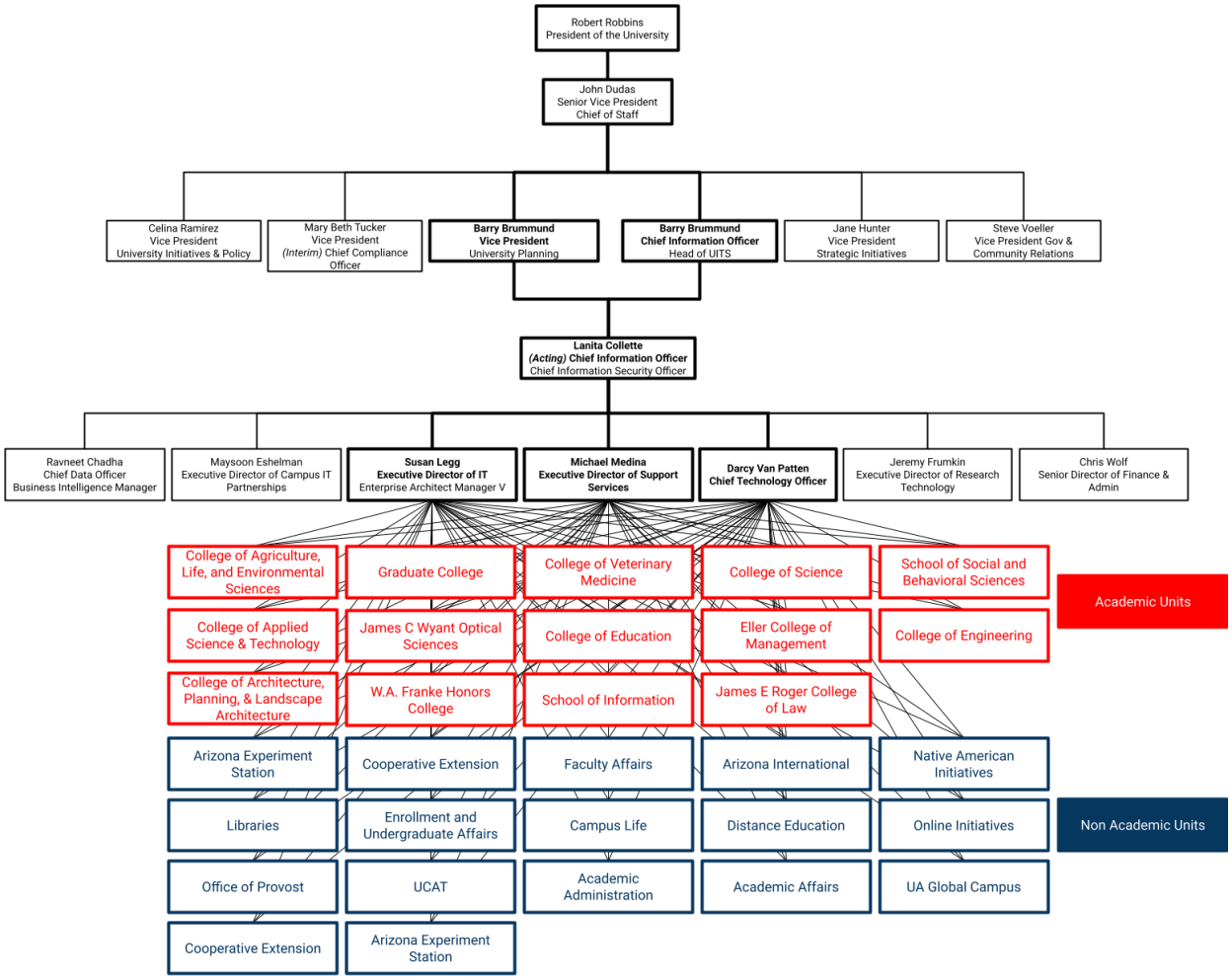


Figure 2: UITS Organizational Chart to be enacted on March 4th. All IT staff from academic (red) and non-academic (navy blue) units now report to one of three senior administrators in UITS (black).

§2 Security

Cybersecurity is one of the primary charges of UITS. Ensuring networks, personal information, communications, financials, research data, and software are protected is critical to the operation of and success of the university's academic and research programs. IT Security is a complex, technical, and mission critical challenge that all modern IT infrastructures must deal with on a daily basis. Attacks can come in the forms of:

- Phishing
- Ransomware and Malware
- Insider Threats
- Data Breaches
- DDoS Attacks

- Advanced Persistent Threats
- Cloud Security Risks
- Mobile and Bring your own device (BYOD) Risks
- Zero-Day Vulnerability

§2.1 Security Audit & 48-month Follow-up

The June 2018 "Arizona's Universities – Information Technology Security" performance audit[31] found UArizona was deficient in 23 recommended areas. The Audit's 48-month follow-up report published in August 2022 found only five recommendations had been implemented, 12 had been partially implemented, and six were still not implemented[32]. Briefly, these were the five areas of concern which UArizona successfully **implemented** post-audit at 24 months[33] and 48 months:

1. Established time frames and guidance for regularly reviewing and updating data inventories (24 months).
2. Wrote IT security policies and guidance documents that explain how UA will guide the management and protection of its IT systems and the data contained in them, such as developing an information security program that outlines its overall approach for selecting, implementing, and assessing the effectiveness of its IT security controls and explains how it will communicate UA's policies and IT security controls to those responsible for implementing them (24 months).
3. Policies and procedures for monitoring the effectiveness of its IT security practices, identifying areas of policy noncompliance, and using monitoring results to inform revisions to its IT security policies and procedures (24 months).
4. Policies and procedures to monitor and assess third parties to ensure that they are adhering to contract or agreement requirements related to IT security (48 months).
5. Communicated the results to UA's leadership (48 months).

And these were the twelve recommendations **partially implemented** at 48 months:

1. Establish security awareness training policies,
2. Revise its security awareness training policies and procedures to require existing employees to complete security awareness training annually,
3. Develop IT security governance,
4. Develop and implement a plan for ensuring its individual units complete data inventories, including establishing a deadline by which all individual units must complete a data inventory and follow-up procedures to ensure all individual units have done so.
5. Conduct the IT risk assessment in all of its individual units,

[31] https://www.azauditor.gov/sites/default/files/2023-11/18-104_Report.pdf
[32] https://www.azauditor.gov/sites/default/files/2023-11/18-104_48-Mth_Followup.pdf
[33] https://www.azauditor.gov/sites/default/files/2023-11/18-104_Report.pdf

6. Compile and analyze the results of the IT risk assessment, and establish a university-wide IT risk profile (based on #5),
7. Develop procedures for assessing whether UA staff are complying with its incident response policies and procedures and take steps to help ensure identified instances of noncompliance are adequately addressed,
8. Develop and implement policies and procedures for training incident response personnel and for testing its incident response process, including establishing time frames for training and testing,
9. Develop procedures for assessing whether UA staff are complying with its incident response policies and procedures and take steps to help ensure identified instances of noncompliance are adequately addressed,
10. Develop and implement additional patch management policies and procedures,
11. Develop and implement additional web application development policies and procedures,
12. An IT security strategic plan that contains a mission, goals, and objectives aligned with UA's overall strategic mission and includes performance measures to assess progress toward achieving those objectives

And these were the six recommendations **not implemented**:

1. Enhance IT security controls to further protect IT systems and data,
2. Develop and implement revised policies and procedures for its vulnerability management process that include requirements and/or guidance,
3. Develop and implement revised configuration management policies and procedures that include the following IT standards and best practices,
4. Developing and implementing additional log monitoring policies and procedures,
5. Developing and implementing university-wide policies and procedures for:
    a. Reporting identified noncompliance with IT security policies and procedures to individuals responsible for implementation and oversight of IT security policies and procedures;
    b. Evaluating instances of noncompliance to determine if and how to address them and documenting why any noncompliance will not be addressed; and
    c. Correcting issues in a timely manner, including developing corrective action plans, providing training, and other steps to address the identified issues, as appropriate, and documenting the corrective actions.
6. Developing and implementing university-wide procedures aligned with best practices that all individual units must follow when developing policies and procedures to address the recommendations in this finding; or include sufficient guidance in its university-wide policies to help ensure its individual units develop procedures for implementing UA's policies that fully align with IT standards and best practices.

Of note, UArizona did not offer "Response Explanations" of how it planned to implement the recommendations to the 48-month review. UArizona only offered the following standard response to all recommendations:

> *"The finding of the Auditor General is agreed to and the audit recommendation will be implemented."*

On the other hand, Arizona State University and Northern Arizona University both provided detailed explanations in their responses.

Relevant to later sections §3, §4, and §5 of this report, the 2018 and 2022 Arizona Auditor General's recommendations[34] makes no references to:

- total IT centralization (including all research units)
- moving operations to a predominantly cloud-based hosting
- hiring an outside company to run IT
- a concern about saving money

§2.2 Arizona Secure IT Services (ASITS)

In March 2023, the Vice President of Research (Cantwell) and CIO (Brummund) announced the Arizona Secure IT Services (ASITS) initiative[35]. The multi-year process that UITS undertook to operationalize the cost of IT and maintain service offerings which support the entire campus is what led the Campus Cloud Infrastructure[36] and is a hallmark of what has become the ASITS initiative.

Another service taking shape before the ABOR Security Audit in 2018 was Managed Cloud Services[37]. Managed Cloud Services allowed other IT groups from campus to take advantage of UITS Amazon Web Services (AWS) resources, operations, and infrastructure transferring local infrastructure workloads into a UITS cloud service managed environment. Another component of what is now called ASITS began with the change to UA network access and adoption of the 802.1x protocol with the Wired Network Registration program[38]. This brought the Secure Network[39] aspect to ASITS[40] which comes with a list of shared responsibilities for stakeholders, colleges and divisions, and members, as well as UITS.

[34] https://www.azauditor.gov/sites/default/files/2023-11/18-104_48-Mth_Followup.pdf
[35] https://research.arizona.edu/announcements/secure-it-services-university-research-activities
[36] https://it.arizona.edu/news/uits-makes-cloud-easy
[37] https://it.arizona.edu/managed-cloud-services
[38] https://wired-registration.telcom.arizona.edu/
[39] https://it.arizona.edu/secure-network
[40] https://it.arizona.edu/about-us/key-initiatives

Around the same time as the change in network access, UITS introduced a new IT Service Management (ITSM)[41] software capability, transitioning from the previous Cherwell Service Desk offering to Service Now[42]. The ServiceNow ITSM is an enterprise class cloud-based solution that UITS employs to provide customer service management, access management, knowledge management, change management, agent workspace, reports and dashboards, surveys, IT operations management and integrations/automations with other systems. Licensing was acquired to allow campus units to use Service Now as their ITSM portal.

The newest addition to the suite of services that was introduced alongside ASITS, as another response to the ABOR Security Audit, is the Technology Lifecycle Care (TLC)[43] which provides unified endpoint management for all enrolled devices. This offering has undergone several changes over the last year and now comes in two versions.

- TLC Enterprise is tailored to colleges with robust IT staffing who would primarily use TLC's inventory, security practices, and device management at no unit cost for the service. Units must refresh their own hardware.
- TLC Extended provides colleges and divisions with a full suite of services that also include user and unit-level support. The cost for TLC Extended is $500 per FTE per year.

There are current uncertainties about how TLC fees will be applied to academic and research departments, student workers, and students.

The final offering that is part of ASITS is the Identity and Access Management[44] solution. Still in the beginning of the implementation phase, the project should provide a more streamlined and reliable central identity and authentication system. Working to create an identity-first security model and develop workflows allowing for improved and more proactive access management and smoother onboarding experience while addressing offboarding needs.

The ASITS plan sets UITS responsibilities in regard to physical infrastructure which includes the campus copper and fiber plan, and intra building cabling, network hardware installation, secure access to telecommunications spaces and on-site infrastructure support.

§2.2.1 Shared responsibility

The shared IT responsibilities of the UArizona stakeholders under ASITS are:

- to comply with UITS policies and classification standards

[41] https://it.arizona.edu/foundational-technologies
[42] https://uarizona.service-now.com/sp
[43] https://it.arizona.edu/tlc
[44] https://it.arizona.edu/identity-access-management

- to secure information on computing resources and intellectual property
- to complete required training defined by the business unit

Colleges and Divisions responsibilities include:

- data classification and data integrity
- data security on end user devices

Members responsibilities include:

- following appropriate compliance guidance
- adhere to all relevant access policies
- define business needs to drive security access rules
- ensure contracts with 3rd party entities/vendors include security clauses (if applicable)
- physical security outside of telecommunication spaces

UITS responsibilities are to provide Security Services for:

- automated threat detection
- patch management
- bug fixes
- code upgrades
- firewall rules configuration
- security incident response

For Infrastructure Services UITS provides:

- Standardized Provisioning Procedures
- Automated backups
- Log monitoring and Management
- Asset Inventory

§3 IT Centralization

Broadly, IT Centralization has been in discussion for over a decade. UITS was itself the result of a centralization of multiple units across campus who performed IT roles in the late 1990's and early 2000's[45] (§1.4).

[45] https://web.archive.org/web/20071231123121/http://uits.arizona.edu/index.php?id=message

Specifically, the current centralization mandate in the 2024 Financial Action Plan[46] follows the announcement of the November 2023 financial crisis. The Office of the CIO also states that centralization is a response to the 2018 Security audit.

On February 14th 2024, emails were sent to supervisors and subordinates that IT would be completely centralized around the University, Cooperative Extension, and the Experimental Stations. On March 4th, over 500 new personnel will report directly to UITS. This will grow the department from ~300 employees to over 800.

As we currently understand it, there will be the three supervisors in UITS with oversight of senior IT employees in Academic and Research who have direct IT reports: Darcy Van Patten, Susan Legg, or Brian Medina (Fig. 2).

Subordinate IT positions will continue reporting to their senior leadership within their assigned units, for the time being. It is not clear if or when future changes will occur in this organizational structure.

Updates to the official UITS website related to centralization[47] are ongoing, with the latest updates still coming almost daily: https://it.arizona.edu/it-centralization/centralizing-information-technology-services

Departmental IT operations will likely begin to transfer to Central IT, who will decide what services move to AWS, and which remain on-premises.

§3.1 Operational Efficiency

The justifications around centralization of IT have shifted over time. Security compliance was identified as the primary reason, a consequence of the 2018 Security Audit and its 48 month follow up (§2.1) (2018-2023). Today, the justification for centralization is communicated as a way of correcting both security problems and the financial crisis (2024) by improving efficiency, security, and financial management:

> "*As part of the University's financial action plan, UITS is centralizing information technology across the institution to create operational efficiencies, standardized processes and procedures, and mitigate cybersecurity risks.*"
>
> – from IT website, February 21, 2024[48]

The implication around operational efficiency is that formerly decentralized IT units within academic departments and research branches are not 100% efficient or their full time employment (FTE) is draining departments' and branches' already limited financial resources. This has been stated without evidence. To the

[46] https://www.arizona.edu/financial-updates
[47] https://it.arizona.edu/it-centralization/centralizing-information-technology-services
[48] https://it.arizona.edu/it-centralization/centralizing-information-technology-services

contrary, UITS financial reports suggest that IT at UArizona is one of the most efficiently run in the country. In FY2020 UITS financial report (page 32)[49], it was highlighted:

> "*In FY20, UArizona's IT expenditure was 6.2%, which was the smallest expenditure compared to higher education peers in all other benchmark categories.*"

In FY2021 reporting (page 22)[50] the IT expenditure number shrank even further to 6.0%, and again in FY 2022 reporting (page 43)[51] to 5.5%. UArizona IT staffing per 1,000 students is also below average compared to our education peers.

To our knowledge, there has been no public or formal assessment of deficiency or financial ineffectiveness of distributed IT responsibilities of academic units or research offices prior to the 2024 Financial Action Plan.

§3.2 Standardization

Standardization of campus IT represents an excellent opportunity to reduce duplicate efforts currently used across the campus IT resources. For example, there are multiple ticketing systems used across campus departments[52]. By moving computing infrastructure onto cloud service providers, the number of systems supported could be reduced or templated using Infrastructure as Code (IaC) tools. Fewer systems could mean fewer system administrators are required to support all systems.

§3.3 Cybersecurity Risks

Recent academic research has found universities with centralized IT have decision making outcomes which are associated with fewer cybersecurity breaches[53]. This is consistent with the idea of a centralized IT having narrower attack surfaces from which attacks can penetrate.

§3.4 Impacts on Stakeholders

Below we detail the impacts of IT centralization to both traditional stakeholders (§3.4.1) and stakeholder groups (§3.4.2).

§3.4.1 Traditional Stakeholders

[49] https://arizona.app.box.com/v/IT-Annual-Report-FY2020
[50] https://live-azs-it-annualreport.pantheonsite.io/sites/default/files/2022-04/UArizona_IT_AnnualReport_FY2021_0.pdf
[51] https://live-azs-it-annualreport.pantheonsite.io/sites/default/files/2023-08/IT_AnnualReport_2022.pdf
[52] https://uagis.arizona.edu/students-faculty/arcgis, https://comhelp.arizona.edu/, https://it.arizona.edu/get-support, https://keating.bio5.org/ticket_support/, https://help.odce.arizona.edu/portal/en/kb/articles/how-to-schedule-a-technician-for-classroom-a-v-support
[53] https://doi.org/10.1080/07421222.2020.1790190, https://penghuang.com/assets/pdf/Cybersecurity-Breaches.pdf

In academic units who had departmental IT support staff (now centralized), personnel often have a domain specific knowledge of the facilities, equipment, software, and research needs of the unit, academic program, and research faculty. This often involves, but is not limited to,

- specific lab-wide hardware installations related to specific research studies
- older equipment that is still in use for data collection, but can only be maintained and operated by computers which have older, no-longer supported operating systems
- Special custom designed instrumentation that is used in a highly specialized environment
- Unsupported, bespoke software, which is not used by any other unit on campus

Departmental IT support personnel often use tools and software that are specific to the units and programs they support, and often these are not supported by UITS.

If centralization results in UITS reorganizing departmental staffing around services and not around audiences and projects, this would most likely result in a significant drop in productivity for any of the scenarios mentioned previously. A central help desk would not have the experience or breadth of knowledge to adequately and responsively provide support when needed.

Some of the largest consumers of IT services on campus are students and faculty through their use in instructional related activities such as classroom and laboratory computers, learning management systems (D2L), etc. While D2L services and centrally scheduled classrooms have had their IT services previously centralized, many departments have their own non-centrally supported departmental classrooms and laboratories that have been built, configured, and managed in a manner specific to the department courses taught in that space. Redesign of these classrooms and laboratories toward a centralized design is an unfunded mandate which will likely incur significant expenses to centralized UITS.

Instructional spaces are often added over time resulting in a wide variety of technologies. The types of personal computer models and manufactures will make a centralized approach with only approved hardware difficult to execute. For example, while there may be one type of video conferencing device in one room, there may be another completely different device being used in another, yet the departmental support person, because of their institutional knowledge, is well versed in supporting all of them seamlessly. This same scenario could be applied to:

- document cameras
- web cameras
- wireless microphones
- wireless presentation devices
- LCDs
- Projectors

Most impactful with centralizing IT support around services rather than audiences is the lack of proximal access to IT support when it is needed. The most common scenario for instructional IT support is a technical issue occurring in the classroom right before, or during a class. There is rarely a lead time given to solve an issue so as to not delay or even cancel class. With departmental IT located in close proximity to the classrooms they support, with the domain and institutional historical knowledge of the environment, it allows for a substantial reduction in downtime for the class, and allows the mission of educating our students to continue with almost no interruption.

Departmental IT support are not just support for instruction, but are instead partners with faculty on classroom technologies, software for students, instructional delivery, and tools for instruction.

Typical routine questions for a Departmental IT support staff person include:

- *"How do I get my students a license/copy of this software?"*
- "*How can I teach students both at a distance and in the classroom?*"
- "*Can you work with a guest speaker to get them connected to our class?*"
- "*Can you help with this software I am trying to use with my students?*"

Because of the integration of IT support personnel within the department, these questions and requests are met in a manner that allows for a quick and appropriate response that allows the faculty to do their jobs and not have to spend time figuring out IT solutions.

There is also a trust and familiarity that comes with a departmental IT person who is an integrated member of the department team, that is often funded partly by discretionary funds in the department, that can never be achieved by a centralization option. In many projects, it has been critical to the overall success of the project that the department IT person has been involved in the planning, execution, delivery, and post-grant work. Continued involvement and connection builds upon itself to further funding opportunities and the security of knowing what can be done, knowing that you have departmental IT support for. These would be unknowns when dealing with a centralized UT unit that may or may not be able to help or prioritize your work.

IT staff also serve multiple functions in departments, ranging from administrative duties, serving as Building Managers, serving on committees, mentoring students, assisting with events, and many others that do not have a role that can be assigned to an UITS service.

IT staff are integrated into their departments so that they can maximize their domain knowledge, provide essential input into a wide range of departmental issues, and assist in the day to day operations of the unit.

Reorienting under a centralization model will impede and in some cases remove the critical aspects of their job and would immediately show a negative return to the unit, who relies on their IT staff for these departmental functions.

Academic departments will need to have flexibility to re-classify the job family of these employees with UITS.

§3.4.2 Research Stakeholders

UArizona is first and foremost the land-grant institution for the state of Arizona[54]. UArizona receives the benefits of the Morrill Acts of 1862 and 1890[55]. The Hatch Act of 1887 added mining and Agricultural Experimental Stations. The Smith–Lever Act of 1914 created Cooperative Extension. UArizona receives funds every year[56] in support of these programs.[57] In FY2023 that financial support was approximately $58.4M.

Second, and no less important than UArizona's status as a land grant institution is that UArizona is in the top 5% of public universities in the country, and is classified as a Research (R1) doctoral university. In 2023, UArizona's research expenditures exceeded $945 million per year for the first time[58].

UArizona is ranked #1 in Astronomy and Astrophysics nationally. Astronomers are major users of campus IT and a primary funding source for recent research computing hardware acquisitions. Supporting the computing and data needs of Astronomy and similar research programs in Health Sciences, Data Science, and Artificial Intelligence (AI) should be the top priorities of UITS.

The Agricultural Experimental Stations, Cooperative Extension, and Research Innovation and Impact (RII) have special requirements which differ almost completely from other IT needs of campus. The unique IT needs of the experimental station and cooperative extension units include the maintenance of a geographically distributed state-wide IT infrastructure[59]. Likewise, the IT needs of RII and research heavy departments (Astronomy, Plant Sciences, Engineering, Hydrology and Atmospheric Sciences) are also unique and include the use of multiple types of computing platforms and data storage which are not met by a single resource provider like commercial cloud.

Steward Observatory, Lunar and Planetary Laboratory, and the NOIRLab receive grants from multiple federal agencies (e.g., NASA, NSF, DOD, DOE) to develop space missions and operate a large number of facilities, include:

---

[54] https://crsreports.congress.gov/product/pdf/R/R45897, https://storymaps.arcgis.com/stories/913da25f6c3d46658690c3800bfef48e
[55] https://cales.arizona.edu/backyards/sites/cals.arizona.edu.backyards/files/b13winter_pp16-17.pdf
[56] https://www.azjlbc.gov/23AR/uniumain.pdf
[57] https://extension.arizona.edu/sites/extension.arizona.edu/files/data/The%20Economic%20and%20Functional%20Impact%20of%20Arizona%20Extension.pdf
[58] https://research.arizona.edu/development/institutional-capacity
[59] https://uagis.maps.arcgis.com/apps/Styler/index.html?appid=1627d784ec2147a18ff51578a9dc83cd

1) Giant Magellan Telescope: $2.5B project of which over $220M in contracts is UArizona
2) Pearl: a $300M project, of which more than $100M is at UArizona
3) NASA Gusto Mission: just completed, a $50M mission
4) NASA Aspeara: $20M, in progress
5) Large Binocular Telescope Observatory (LBTO): ~$14M a year; international and national partnerships including Italian National Observatory, the Ohio State University
6) Multiple Mirror Telescope (MMT): ~$2.5M a year; partnership with Smithsonian Institution
7) Magellan Telescopes: a $8M a year enterprise, UArizona is a 10% share

The "Cyber Experiment Station"[60] within the CALES manages IT at Cooperative Extension offices and the Arizona Experiment Station locations in both Arizona and New Mexico. Outreach at each site is different, depending upon local stakeholders. These vary from vegetable farming in Yuma, grain and cotton in Maricopa, to beef producers in Kingman, all the way to Shiprock NM. The Cyber Experiment Station creates applications which are then passed by Cooperative Extension Agents directly to the rural stakeholders and are critical to fulfilling UArizona's mission as a Land Grant University. The IT has essentially already been centralized within the Experiment Stations, at least since the introduction of dual-factor authentication was required by UITS. Connections are authenticated via wired network registration and requires UITS to have visibility on every port terminal to every computer. The Experiment Station has helped to connect high speed fiber in Yuma, and is beginning to adopt StarLink (low-earth orbit satellite internet) in other locations including Payson. This critical infrastructure improves UArizona competitiveness for research funding and helps attract commercial partnerships.

Cooperative Extension's Tribal Extension[61] works with Tribal partners through the Federally-Recognized Tribal Extension Program (FRTEP)[62]. Further, the 22 federally recognized tribes in Arizona[63] have sovereignty over their data which is maintained over tribal lands and they maintain their own IT infrastructure independent of UArizona.

§3.4.3 Specific Impacts to Research Infrastructure

Centralization of IT in previously decentralized IT infrastructures may lead to an endangerment of life and property. Examples of decentralized IT resources which control purpose-built equipment and facilities[64] at:

- Telescope sites

[60] https://cct.arizona.edu/
[61] https://extension.arizona.edu/tribal-extension
[62] https://www.nifa.usda.gov/grants/programs/nifa-tribal-programs/federally-recognized-tribes-extension-program, https://tribalextension.org/
[63] https://statemuseum.arizona.edu/native-nations-arizona
[64] Richard F. Caris Mirror Lab, UA Tech Park, Large Fiber Array Spectroscopic Telescope, Giant Magellan Telescope, PERL, Machine Shops, Steward Observatory Radio Astronomy Lab, Magellan Adaptive Optics X, Event Horizon Telescope, Arizona Robotic Telescope Network, James Webb Space Telescope, NEID, Mountain Operations, Multiple Mirror Telescope, Arizona Radio Observatory, Center for Astronomical Adaptive Optics

- Technology Integration Centers
- Research Labs

These locations are highly specialized and require full time dedicated IT staff to manage. Variously, these sites also require decentralized IT controls to meet federal contracting requirements and to guarantee mission success.

A loss of control on security in IT resources at these sites could result in violations around,

- Documented CMMC Level 1 policy and procedures for onsite systems as requested by contracts[65]
- Disruption to established procedures for ensuring physical access
- Failure to conduct annual safety reviews which may be evaluated by personnel lacking requisite experience
- ITAR specific system encryption tools & procedures which require secure:
    - storage locations
    - encryption strength
    - key storage
- ITAR compliance that requires intimate knowledge of systems and training
- Disruption in periods of critical support (24/7 availability, e.g., Telescope mirror casting)
- Reduced response time for onsite support requests for failures in hardware, data drives, and network connectivity

Concerns around centralized IT also relate to it being less likely to have the current extensive proactive monitoring tools, e.g., Zabbix, Grafana, NUT-UPS, for real time monitoring, text alerts, performance history, for systems/networks/environmental conditions.

As an example of a central point of failure with existing IT security, the December 14th 2023 security breach was because NetIDs were stolen following a malicious email that went through and not because of unpatched systems.

Further examples which could result in a loss of project effectiveness:

- Knowledge of specific departmental software requirements[66]
- Loss of access to preferred project management tools (e.g., long term SLACK use for inter-organizational projects)
- Configured resources according to the needs of specific research group
- Intimate knowledge of networking information resources might be lost

[65] https://dodcio.defense.gov/CMMC/Assessments/
[66] Legacy IDL, Licensing for IDL, ANSYS, Solid Works, PDM Vault, ITAR software, IRAF, GILDAS

§3.4.4 Past Experiences with Central IT

Some anecdotal examples of previous interactions with Central IT from Campus IT groups that were provided to the committee are included below, the quotes have been edited for clarity:

- "*Delays in the approval of non-standard computers (i.e., Linux OS servers, and other brands of laptops), which required substantial paperwork including signatures from Department Heads and Deans to purchase.*"

- "*All computers were shipped from the vendor to Central IT where they installed various remote access software. Researchers recalled "scanning" programs that were searching for personally identifiable info, as well as auto-updated software, and software that would occasionally (i.e., in the middle of the night) try to phone home and consume large CPU and network resources. This caused problems with instrument computers and took a significant effort to figure out how to remove the problem applications, in part because Central IT would not tell research teams what had been installed. Researchers have wiped and reinstalled the OS after delivery to remove these problems.*"

- "*IT support requests were received by a changing group of IT people. So if you filed a ticket on a long-standing issue, it would go to someone who did not have the "history" of the problem, and essentially was starting from scratch.*"

- "*Support staff at Central IT are knowledgeable and experienced and have been working directly in departments, but they were blocked in what they could do or say by Central IT management. The size of the IT workforce was also reduced, while workloads increased, so that people had time to only superficially engage on problems, which was counter to the very involved way that many departmental IT units now operate.*"

§3.5 What are the driving forces behind IT Centralization and ASITS?

The Arizona University's Information Technology Security audit identified 23 recommendations to the University of Arizona for improving IT security (§2.1). The audit recommendations became the basis for some of the foundational pieces of the ASITS program.

In June of 2021 ABOR proposed a list[67] (page 24) of annual, incentivised goals to President Robbins, among those a $25,000 salary bonus to:

[67] https://www.azregents.edu/sites/default/files/2023-04/Sept.-Oct._%202021_board_book.pdf

> "*Implement a new budget model to replace Responsibility Centered Management (RCM) and develop and begin implementation of a plan to reduce college and department overhead costs ("Academic Support") by at least $10 million through the appropriate centralization of support services like Information Technology, Human Resources, Finance, Marketing, Communications, Fundraising, and Advising.*"

The November 2022 ABOR (page 73)[68] set performance incentives for President Robbins were:

> "*By June 30, 2023, develop, adopt and communicate a plan to centralize responsibility and balance local authority in the university-wide administrative functional areas of Information Technology and Financial and Business Services. The plan should include appropriate transfers of budgetary, financial, hiring and operational accountability to maximize service, effectiveness, and efficiency.*"

> "*Implement and document an Information Technology security governance framework that includes: an IT security strategic plan, articulated roles and responsibilities, policies and guidance, training across the university in security awareness, and processes for monitoring and evaluating the effectiveness of institutional IT security practices.*"

Critically, the above statements refer to the centralization of responsibility in functional areas of IT and Financial and Business Service but not to technical hardware or software centralization, as applied to research and academic activities.

In August 2022, the 48-month follow up to the initial [Arizona Auditor General] audit report identified 6 recommendations that were not implemented, and another 12 that were partially implemented (§2.1). During this time, President Robbins and the UA Senior Leadership Team were being advised on IT security by the CIO (Brummund) in a manner which was inconsistent with the reality on the UA Campus, as presented by then-Provost Dr. Liesel Folks:

> *"Here is what I lose sleep over. I have been told by Barry Brummond that we are 10 years behind in IT security on this campus,"*
>
> – Provost Liesel Folks "Live Chat with Liesel and CALS," November 15, 2022

In October 2022, Central UITS presented to the campus IT community a list of mandates centered around new IT services for the University. The Accelerating Secure IT Services for Campus Units (ASITS) plan proposed a nearly complete transfer of service responsibility from campus units to centralized IT.

---

[68] ABOR. "November 16-18 2022 Board Book." *Arizona Board of Regents*, November 2022, https://arizonastateu.sharepoint.com/sites/O365ABOR/public/Committee/Board/Shared%20Documents/Forms/AllItems.aspx?id=%2Fsites%2FO365ABOR%2Fpublic%2FCommittee%2FBoard%2FShared%20Documents%2F2022%2D11%2D16%2Dthrough%2D18%2DFinal%2DBoard%2DBook%2Epdf&parent=% Accessed 1 March 2024.

Critically, the ASITS plan does not explicitly relate to conclusions of the 2022 48-month ABOR follow-up audit. ASITS would however completely change IT operations on the UA campus.

The following communication was sent to UITS leadership on October 24, 2022 from campus IT managers to the CIO (Brummund). In the message the IT managers are expressing concern over the planned implementation of ASITS:

> "*We would like a better understanding of how staff positions are being handled and what options are being made available to employees whose relevance may be reduced or eliminated by the proposed changes. The abrupt way this plan was announced has had an intense emotional impact on staff across campus,*"
>
> – email from Campus IT Managers to CIO Brummund, October 2022.

It is important to note at the beginning of the current IT Centralization, that particular concern was not considered, particularly in "*The abrupt way this plan was announced has had an intense emotional impact on staff across campus.*"

By Spring 2023 there had been significant pushback around ASITS from campus groups, in particular Faculty Senate and University Research Faculty. After a near full year of investigation, reporting, and evaluation, much of the ASITS plan and in particular the TLC had not been implemented, or only on a very small scale.

Remarkably, funding for ASITS was not allocated into FY 24 budget, so there was no additional funding for implementing the Technology Lifecycle Care (TLC)[69] program, as originally intended, and the cost analysis of the cloud services migration was not released. However, ABOR and the Office of the CIO have continued the push for total IT centralization.

After the announcement of the financial crisis in November 2023 and the resultant Financial Action Plan, the new "plan" for centralization of IT services was revived in February 2024 with three weeks notice.

The IT Centralization plan was not tied back to ABOR security recommendations of 2022. Instead, it was re-announced as part of the University's plan to cut costs and improve efficiencies. The amount of those costs, and the examples of inefficiencies were not given.

Misrepresentations of the state of IT security on campus have also been used to justify IT centralization:

> *"You know, we have inconsistency [in] management of our IT issues across this campus and that has led to a couple of things. One, some disruptions in the security of our information technology.*

[69] https://it.arizona.edu/tlc

Barry can talk for hours and give 427 examples off the top of his head of IT breakdowns that we need to solve, so that in number one, we have security issues.

Number two, we have cost issues around IT.

And it's not in the professionals, it's in the way we're procuring IT and managing IT."

– John Arnold, UA Interim Chief Financial Officer

The case has also been made that the effort for IT centralization had little to do with directly addressing the security audit recommendations, and has more to do with achieving financial incentive goals set for President Robbins.

At the September 28-29, 2023 meeting, a financial incentive was given to President Robbins:

"By June 30, 2024, complete centralization of Information Technology Services. Failure to implement the plan will result in a reduction of $20,000 from the total at-risk compensation awarded for 2023-2024."
– Arizona Board of Regents Meeting, September 28-29, 2023. https://tinyurl.com/2zrerjej

If thoughtfully planned, reviewed, and methodically implemented, the IT centralization may yet achieve a $10M in savings and net President Robbin's financial bonus incentive.

§3.6 Strengthening and Justifying ASITS in UITS

The UITS centralization may be used to justify increases in both revenue and expenses into the Office of the CIO. Importantly, this will also provide funding for and mask the full financial investment needed to finally implement ASITS. Central IT had increasingly relied on Campus IT to implement its programs (see Wired Network Registration (WNR)[70] and BLUECAT migration[71]) expending Campus IT resources for implementing the unpopular ASITS plan.

During the implementation of Wired Network Registration, hundreds of customer premises equipment network switches were removed and replaced with managed CISCO switches. For some campus department data center switches funding from Central IT was not provided with the justification that funding was no longer available.

[70] https://uarizona.service-now.com/sp?id=sc_cat_item&sys_id=ac521541db347c109627d90d689619c8
[71] https://itsummit.arizona.edu/bluecat-migrations-learn-experience, https://bluecatnetworks.com/blog/our-process-for-a-successful-bluecat-migration/

The TLC program was also scaled back to no longer include campus-wide IT support. Campus IT were responsible for hardware replacement, implementation, and monitoring of the security tool Workspace One[72].

These changes in course from the original ASITS program raise the question: is improved security really the reason why we need centralized IT? Or is IT centralization the goal, and the Financial Action Plan provides the opportunity?

§4 Cloud Services

Cloud computing began in the early 2000's and commercial cloud service providers were beginning by the early 2010's. UArizona IT was an early adopter of cloud, and has been at the forefront of cloud computing and cloud infrastructure integration for over ten years.

UArizona IT was one of the first, and is now one of the largest, consumers of commercial cloud services in the country[73]. UArizona uses cloud services for most of its administrative and security functions. Arizona's Cloud First policy encourages the adoption of cloud technologies whenever possible[74].

§4.1 Migration to Cloud

UArizona IT began its migration to cloud services in 2013 culminating in an award for leadership in cloud in 2017 (Fig. 1)[75].

Under the direction of CIO Brummund, UITS has led a transition of the University's core services to a commercial cloud provider, Amazon Web Services (AWS). AWS is the largest cloud computing provider in the world[76]. They are also Amazon's most profitable unit[77]. The choice of AWS was logical in parts because of their availability and well developed portfolio of services.

UArizona currently uses AWS managed Cloud Database Services to provision secure instances of MySQL, PostgreSQL, Oracle, and MS SQL Server databases, that comply with regulations like FERPA[78]. UArizona also operates Controlled Unclassified Information (CUI)[79], ITAR[80] in the AWS GovCloud[81], which supports

[72] https://techzone.vmware.com/resource/workspace-one-cloud-services-security
[73] https://aws.amazon.com/solutions/case-studies/university-of-arizona/, https://it.arizona.edu/news/uits-makes-cloud-easy
[74] https://aset.az.gov/resources/cloud-resources
[75] https://it.arizona.edu/news/ua-wins-cloud-leadership-awards, https://www.annualreport.it.arizona.edu/2018-cloud-services, https://aws.amazon.com/solutions/case-studies/university-of-arizona/
[76] https://dgtlinfra.com/top-cloud-service-providers/
[77] https://www.constellationr.com/blog-news/insights/aws-q4-revenue-growth-13-amazons-results-shine
[78] https://it.arizona.edu/news/uits-makes-cloud-easy
[79] https://research.arizona.edu/sites/default/files/cui_faq_01.11.2021_0.pdf
[80] https://rgw.arizona.edu/sites/default/files/faqs_01.11.2021_1.pdf
[81] https://aws.amazon.com/govcloud-us/

security requirements for those projects. AWS cloud services meet with the security mandates required of working with these data, relieving UITS of the requirements of managing the hardware and networking. Additionally, CyVerse Health (Soteria)[82] operates on AWS HealthCloud[83] to meet its security mandates around HIPAA[84]. The student CatCloud[85] is also managed by AWS.

Commercial cloud providers (including AWS, Microsoft Azure, and Google Cloud), all use fine-grained cost models with pricing for every service and associated functionality. Some of these include:

- **Data Ingress:** The cost of uploading data to the cloud. Large datasets are actually too big to move over the internet and require physical transfers to cloud service centers.
- **Data Storage:** The cost of storing data in the cloud. There is a wide range of tiered storage options with rates which vary across providers. Rates are lower for less accessible data (larger latency).
- **Data Egress:** The cost to transfer data out of or across clouds. Data can be used within a specific regional cloud service, e.g., AWS West-1 S3[86] datasets are processed on AWS West-1 cloud EC2 instances.
- **Compute:** The cost to do science in the cloud. Resource use is billed as a function of time, with larger resources like GPUs for AI and machine learning costing the most.
- **Serverless/Functions:** The cost to do science in the cloud. A vendor cost model where the cloud provider manages dynamic event-driven functions, on a per-call basis.
- **API Requests:** The cost to do science in the cloud. A vendor cost model where the cloud provider manages the API and charges users per API request.

It is important to understand how these fees, pricing, and costs apply to services. In order to gain a financial benefit and to incentivize users to not 'waste' computing resources when they are not in use, IT managers need to have a deep understanding of both the billing and the operations of cloud deployments.

§4.2 Cloud Benefits

Commercial cloud has many benefits which increase its operational effectiveness and the economics of UITS.

Centralizing IT under UITS has several benefits, and relative cost savings which align with budgetary conservatism. By managing IT decisions centrally UArizona can limit duplicative efforts to deployment and configurations across academic departments.

---

[82] https://soteria.arizona.edu/

[83] https://aws.amazon.com/health/

[84] https://research.arizona.edu/compliance/hipaa-privacy-program

[85] https://edscoop.com/university-arizona-catcloud-student-designed/

[86] https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Concepts.RegionsAndAvailabilityZones.html

Scenarios where commercial cloud providers are beneficial over on-premises server management:

- Reduce footprint of local infrastructure (building square footage, cooling, power, etc.), and physical IT staff for managing hardware and software.
- Paying only what you need using spot or on-demand services.
- Mitigated risk via a new off-site backup location.

Scenarios where commercial cloud providers are beneficial, specific to research computing:

- Avoid long queue-times or maintenance windows for local resources (HPC, servers, etc)
- Execute large, independent workflows or workloads.
- Availability of the newest (<1 year old) hardware architecture

§4.3 Cloud Vendor Lock-in

Amongst the risks and pitfalls of commercial cloud providers, we want to highlight two areas: the possibility of so-called 'vendor lock-in', and inefficient use of cloud resources in particular for data storage and data egress.

A major concern in the use of commercial cloud is "vendor lock-in" whereby specific cloud providers' bespoke features become requirements for managing and operating a large deployment, like what the university has established. Below we offer potential risk-factors and mitigation strategies identified in the 2024 National Science Foundation (NSF) Major Facilities Cloud Use and Considerations publication[87].

Risk factors for vendor-lock in are:

- **Data transfer** - beware of asymmetric pricing for data ingress versus data egress.
- **Applications** - beware of using vendor specific APIs for university managed applications.
- **Human Resources** - training employees to use one cloud is expensive and labor intensive, re-training or training new employees is also time consuming.
- **Security / Authorization** - vendors use their own authentication systems which must be built for bespoke user deployments
- **Costs** - vendors offer introductory or negotiated discounts which can be changed without consultation. Vendors can also modify pricing based on usage just enough to keep you from switching.

After the customer is 'locked in,' a vendor could end support or discontinue features which are not profitable, or update their pricing by increasing usage rates or storage costs. In both cases the customer (the university) is

[87] https://doi.org/10.5281/zenodo.10481410

unable to negotiate the same deal as before (or negotiate a lower price) and must now begin an expensive migration to another cloud service provider.

Data storage on the cloud can also become an issue when datasets are very large, as is the case for many types of research data, e.g., image or video data from medical devices, remote sensing data, genomic datasets, AI training datasets. The cost of storing, hosting, and providing egress of large datasets from commercial cloud providers can be an expensive proposition which may impact limited or set budgets for academic departments, libraries, or research awards. Issues around data security, data backup (redundancy or off-site hosting) also increase costs.

$4.4 Cloud Services for Academic Units

A required move by Campus IT to AWS could impact existing workflows to research faculty, not just in a change of process or procedures, but in the temporal investment of how to make it work, even if it was possible.

For some projects, proximal access to the data, and storage, is a mandate for the success of data collection. Taking into account lag-times and other network delays, depending on the nature of the research and data collection it simply may not be possible, or the requirement to find an accessible solution be too time consuming and disruptive to be feasible.

In addition to established research projects already having specific workflows in the context of using existing on-prem storage and the disruption that moving, mid-project to a cloud storage solution there are other considerations which make a proposed migration to cloud services a burden for faculty in small to medium size units.

Faculty who have been contracted to use outside or third party data sources often must submit a data management plan, detailing how the data will be stored, who will access, how it will be accessed, and how it will be destroyed at the conclusion of the project. For many agreements, satisfactory responses to these requirements are often the determining factor in whether access to a data set is granted.

An example can be found in the data access requirements for the Inter-university Consortium for Political and Social Research, at the University of Michigan. As part of their application requirements to access data sets, included in the application requirements is the following:

> "*Confidential Data Security Plan: Applicants will select a confidential data security plan and agree to all terms included therein. The fundamental goals of this plan are to ensure that the restricted data are stored securely and are accessible only to the people listed in the application. ICPSR offers three confidential data security plans for secure download data: External hard drive, non-networked computer, and local virtual or physical enclave on an isolated network,*"
>
> – (https://www.icpsr.umich.edu/web/pages/ICPSR/access/restricted/).

Any requirement for cloud storage for University of Arizona research faculty using such a dataset would preclude their access to the data and not allow for the use of that dataset.

In the context of research faculty in a small to medium size department, often there is just the Principal Investigator, a graduate student, and maybe a small team of undergraduate research assistants, and perhaps a paid University Staff Research Associate. These are not large operations, and funding is accounted for down to the last dollar to maximize the scope of the research. Existing projects would have no budget to fund a mid-project move to a cloud storage solution. New projects would potentially have their budget consumed by cloud storage costs, especially as compared to existing on-premise solutions.

There is also the concern that funding agencies, when looking at the cloud services requirements being applied to research faculty may not choose to grant our faculty the external funding, because the agencies may get a better return on their investment from institutions that do not have such requirements. Faculty in small to medium size departments are already stretched thin with increasing teaching loads, increasing course caps, and now perhaps the increased burden of having their research appointment be put in jeopardy because of these cloud computing requirements. Together these form an undue burden on existing and future research projects.

§4.4.1 Cloud for Teaching

Academic departments and course instructors perform a significant amount of technical work. Depending on the subject matter and skill level it is atypical for the enterprise services that UITS currently offers to be sufficient for course assignments and student assessments. Instructors may also require services that are more specialized. Those instructors that have good IT personnel available to them through their department or college may work with those individuals on operations and infrastructure, to ensure courses go well and are a good experience for their students. Instructors who do not have IT resources available to them are likely doing this IT or IT-like work themselves. Instructors who are working with centralized IT now may be faced with having to redesign their courses and perform more of this work themselves if the IT effort available or priority levels change.

Departments also rely on academic software license programs, which can provide Commercial-Off-the-Shelf (COTS) software products to faculty, staff and students for free or for minimal costs. The software titles of interest to our members are often industry standard in a given sector or area of expertise, and our students benefit greatly from their exposure to these titles. Some of the agreements we have in place to administer or fund such agreements are ad-hoc or informal, sometimes several like-minded departments across the institution coming together to fund a particular agreement, with parties exiting or entering over time. It would be ideal if any centralization or cost-saving effort looked at preserving these agreements and maximizing their use. Instead, there have been attempts by UITS to restrict the catalog of software offerings in situations where an agreement is seen as duplicative of an existing agreement. But the decision on which software to use for a course should generally be driven by the instructor and their department, responding to student needs and perhaps by industry

demand. Additionally, some of these license programs have specific restrictions on which devices they may be installed on, and may require limits on access. As a result, some are only feasible on a small scale, like a departmental lab, or on on-premise hardware that is owned by the institution. This can be complicated further by courses that cross modalities, including course courses where students are interacting with servers to complete their work, or by online students who remote in to use institutional resources to complete their assignments and assessments.

§5 Research Computing & Data Storage

Research Computing at UArizona takes place both within academic units and within Central IT. Research computing requires its own section, in particular, given its utilization of both cloud services and on-premises computing resources and data storage.

Research Computing includes the High Performance Computing (HPC) center located at the UITS Building.

Over the last 30 years, UITS and RII have contributed annual funds as a 'set aside' for purchasing the next high performance computing (HPC) hardware. This has allowed the university to purchase a new HPC at least once every three to five years. From 2017 onward, that set-aside was re-allocated to other purposes. Decisions were made between the CIO (Brummund) and Vice President for Research (Cantwell) to use those HPC funds to purchase needed enterprise software licenses. First to address research administration system upgrades and then to support core research computing staffing that was previously funded through the UITS budget. This decision was made without consultation with the HPC community users at UArizona, and has resulted in significant confusion and frustration from UArizona faculty and staff.

UArizona research computing is world renowned for its science with international acclaim for projects like the Event Horizon Telescope (EHT), OSIRIS-REX, the Vera Rubin Telescope, and CyVerse. Specifically, the first image of a black hole produced by the EHT team would not have been possible without the HPC facility and collaboration with UArizona staff working on national cyberinfrastructure projects like the OpenScienceGrid HTC.

§5.1 Research Computing

Modern scientific research has very specific computing and data hosting requirements. These requirements are not necessarily met by a single solution, such as commercial cloud hosting.

In 2018, 15% of UA's total sponsored research projects relied upon the HPC services[88]. By 2022, that number of principal investigators has more than tripled, and the expenditures in research dollars has increased nearly six times (Table 1).

[88] https://arizona.app.box.com/v/UITS-Annual-Report-FY2018

Table 1: Total numbers and research awards ($ millions) for research computing (data from UITS annual reports). 2023 is not available yet.

Year	2018	2019	2020	2021	2022	2023
Expenditures ($ Million)	67	196.7	212	395	382	n/a
Principal Investigators (#)	180	572	426	449	580	n/a
Root Award (#)	657	815	1,481	1791	1800	n/a
Researcher (#)	n/a	n/a	926	1545	n/a	n/a

In 2021 and 2022 campus HPC resources supported $395M and $382M in sponsored research expenditures, respectively[89].

Currently, UArizona does not operate enough GPU computing resources to operate as a top tier AI research university. Our existing GPU capacity is too low to teach large classes in AI, or to do substantive AI related research, such as training our own large language models (LLMs) or self-hosted deployments of private LLMs which are secure and use sensitive or proprietary data and can be used internally be University faculty and staff for research and administration.

§5.1.1 High Performance Computing

The Research Technologies Department provides campus researchers with High Performance Computing (HPC) clusters, storage resources, and consulting services for research purposes. These resources complement and extend college and departmental resources in order to provide the UA faculty with a range and depth of cyberinfrastructure appropriate to their research. The staff provide support from getting started to building complex scientific software and data visualization. These services are open to any faculty, researcher or student who has a use for HPC systems.

§5.1.2 Co-location

UITS operates a co-location space, the UArizona Research Data Center (RDC), where faculty can buy-in with their own hardware purchases. As part of the larger centralization plan, the co-location space would be a logical place for researchers to transition their departmental servers.

The physical infrastructure is housed at the RDC which is a restricted access facility with redundant power, cooling, and 24/7 monitoring.

[89] https://www.annualreport.it.arizona.edu/sites/default/files/2022-04/UArizona_IT_AnnualReport_FY2021_0.pdf

Recently, UArizona closed the USA Building, previously the building had been used as an off-site backup and disaster mitigation location for data storage.

§5.1.3 High Performance Computing reinvestment fund

The last HPC renewal funding announcement and committee work was done in 2019, which resulted in the 2020 deployment of Puma[90]. Recently (February 2024), it was announced that RII had procured ~$5M in TRIF funding for the acquisition of a new HPC, in continuation of the HPC refresh which has been going on since 1990's.

§5.2 Data Storage

Currently, research data are stored on a variety of servers and cloud services distributed across academic and research units. The UArizona Libraries Data Cooperative maintains a list of data storage and data backup solutions[91] which include archiving and data storage, backups and security.

For years, UArizona staff, students, and faculty have been using cloud-based data storage options, many provided free of cost.

Current UArizona data Storage, Back-ups & Security Solutions include:

- Box (50GB)
- BoxHealth (50GB)
- One Drive (1TB)
- Google Drive (15GB)

The HPC center also includes multiple research data storage options[92]:

- Tier 1 (50GB/500GB/20TB)
- Tier 2 (1TB)
- Rented Storage ($48/TB/yr)
- Buy-in (133TB)

UITS offers two tiers of storage managed through AWS[93].

[90] https://it.arizona.edu/news/high-performance-computing-updates-mean-more-compute-time-researchers
[91] https://data.library.arizona.edu/data-management/best-practices/storage-back-ups-security
[92] https://uarizona.atlassian.net/wiki/search?text=Storage&spaces=UAHPC, https://uarizona.atlassian.net/wiki/spaces/UAHPC/pages/75989618/Storage
[93] https://uarizona.atlassian.net/wiki/spaces/UAHPC/pages/75990099/Tier+2+Storage

Long term archival storage is intended for data used in publications and in support of research projects. Archival data hosting varies by size[94]

- ReDATA[95]
- CyVerse Data Commons[96]

CyVerse[97] has done an extensive cost-benefit analysis of its multi-petabyte data store hosted at UITS in the co-location and mirrored nightly at the Texas Advanced Computing Center (TACC). Moving it's storage hosting from UITS to a commercial cloud provider (e.g., AWS S3), would exceed $10 million per year in operating costs, not accounting for data egress fees. Comparatively, CyVerse's entire operating budget including staffing is ~$3.5 million per year.

Data security for regulated, protected, and secured record data[98] includes use cases for:

- IRB
- FERPA
- HIPAA – RedCAP, BoxHealth

Research Data Storage Service back-up data tiering is available[99]

§6 Recommendations

In conclusion, we summarize the information above in §2, §3, §4, and §5. The following recommendations are intended for the Faculty Senate to discuss with the Office of the CIO as a means of co-production. Our suggestions relate to where we feel a Centralized UITS is best positioned to improve services and opportunities for UArizona students, faculty, and staff as stakeholders.

§6.1 Improving Shared Governance

Shared governance at the University of Arizona aims to ensure informed decision-making and is based on the laws, policies, and statements outlined in Arizona Revised Statute §15-1601(B)[100], Arizona Board of Regents Policy Manual -Conditions for Faculty Service[101], University Handbook for Appointed Personnel[102],

[94] https://data.library.arizona.edu/data-management/best-practices/data-sharing-archiving#UA-archiving
[95] https://redata.arizona.edu/
[96] https://datacommons.cyverse.org/
[97] https://doi.org/10.1371/journal.pcbi.1011270
[98] https://research.arizona.edu/sites/default/files/data_security_and_records_retention_v2020-04.pdf
[99] https://uarizonadev.service-now.com/sp?id=kb_article&sys_id=13f5ea5b97487194b41055b00153af05
[100] https://www.azleg.gov/ars/15/01601.htm
[101] https://public.powerdms.com/ABOR/documents/1499253
[102] https://policy.arizona.edu/employment-human-resources/role-appointed-personnel

Constitution of the Faculty of the University of Arizona[103], and American Association of University Professors (AAUP) Statement on Government of Colleges and Universities[104].

On May 13 2022, in a letter accompanying the Shared Governance Memorandum of Understanding (MOU)[105], jointly signed by the President, Faculty Senate Chair and Vice Chair, and the Provost, President Robbins wrote:

> *"Of course, effective shared governance must include all campus stakeholders — including staff and students — and our faculty and administrative leaders are committed to soliciting input and expertise across all constituencies to, as the document suggests, leverage our collective wisdom."*

The above referenced MOU also states:

> *"Shared governance includes solicitation of input from all stakeholders on campus including faculty, staff, students, and administrators - and honoring the expertise and lived experience of all of us. This leveraging of our collective wisdom, with faculty and administration particularly committing to open channels of communication with staff and students, frequently requires ad hoc committees that represent different constituencies and focus on particular issues and timely concerns."*

Therefore, it is essential for all stakeholders to be engaged in the decision-making process that involves IT services on campus.

§6.2 Security

To protect and mitigate against these risks UITS must implement multi-layered security strategies which include security awareness training for all, robust access control, vulnerability assessments, penetration testing, incident response planning, and security updates.

§6.2.1 Benefits and Opportunities

By consolidating IT resources and governance under one framework, UArizona can achieve uniform control over its cybersecurity measures, facilitating better strategic planning and swift implementations of security protocols.

§6.2.2 Risks and Pitfalls

[103] https://arizona.app.box.com/s/r8ndupxl34xz5ori3lq1mx8l3v4et6bu

[104] https://www.aaup.org/report/statement-government-colleges-and-universities

[105] https://facultygovernance.arizona.edu/sites/default/files/2022-08/Shared%20Governance%20Faculty%20Letter%20and%20MOU.pdf

By centralizing IT, we risk creating a single point of failure within the IT infrastructure, which could be catastrophic if breach or system failures occur. While centralization is aimed at security measures, it may also slow the institutional ability to adapt to department-specific needs or emerging threats. There is also a challenge to the implementation of diverse systems of technology and systems which complicate the security landscape.

§6.2.3 Mitigation and Alternative Approaches

We encourage a hybrid approach to the centralization of IT security. A hybrid approach could include: high level security policies and protocols which are governed from Central IT, while allowing individual departments and research units the autonomy to implement additional specific security measures tailored to their needs. This can address the single point of failure problem identified above.

Engaging in regular cross-department consultations through the creation of an advisory council or committee can foster a more integrated IT security framework. Sharing of best practices and swift identification of and adaptation to new threats is critical.

§6.3 Centralization

In the opinion of this committee, the IT staff of UArizona are some of the most important, dedicated, and hardworking employees of the university. Without their daily work in IT, our modern university would cease to function. Our daily lives are kept safe by the security measures provided by our IT and our communications, teaching, and research are all made possible by the networking and computing and data infrastructure provided by our IT system.

The initial planning and execution of the 2024 UITS centralization effort was planned and executed in private, without the consultation of Department Heads, Vice Presidents, or IT Stakeholders. This has led to issues around violations of federal contracts, uncertainty in operations, disrupted planning around new IT acquisitions, maintenance of existing systems, and a general loss of morale.

While Centralization has been pitched as the solution to our IT problems, little attention has been given to the benefits of Decentralized IT solutions. For the Faculty Senate's reference, we include the findings of Liu et al. (2020)[106] who studied the effects of centralization in IT across 504 US institutions of higher education over a four year period. Below in Table 2 we summarize the results of Liu et al. (2020) and present both Centralized and Decentralized benefits and weaknesses.

Table 2: Liu et al. identified aspects of IT centralization and decentralization across 504 US institutions.

[106] https://doi.org/10.1080/07421222.2020.1790190

Aspect	Centralization	Decentralization
Benefits	- Uniform control - Strategic planning	- Swift decisions - Promotes autonomy
Risks	- Slow to adapt to specific needs	- Fragmented policies - Inconsistent standards
Pitfalls	- Single point of failure	- Difficult integration - Increased complexity
Governance	- Easier policy enforcement - Centralized decision-making	- Local autonomy - Flexible decision-making
Efficiency	- Streamlined processes - Consolidated resources	- Quick local responses - Adapts to specific needs
Security	- Unified security protocols - Easier to monitor and control	- Diverse approaches can complicate oversight - Tailored local solutions
Innovation	- Potentially slower due to bureaucracy - Innovation at scale	- Faster local innovation - Encourages experimentation
Cost	- Potential for economies of scale - May have higher upfront investment	- Possible redundancy in spending - Lower initial investment
Risk Management	- Central point of vulnerability - Efficient risk assessment	- Diffused risk - Challenges in centralized risk management
Scalability	- Planned, uniform scaling - May be slow to adapt	- Scalable in segments - Flexible adaptation to changes
Integration	- Easier integration of systems and policies - Uniform IT landscape	- Complex integration of disparate systems - Potential for incompatibility

§6.3.1 Benefits and Opportunities

UArizona will benefit significantly from enhanced alignments and resource optimization through centralization. Centralization offers unified approaches to IT governance (Table 2), establishing coherent university-wide policies and standards that streamline operations and reduce redundant systems. Centralization will also enhance cybersecurity measures through uniform security protocols and practices, strengthening overall university defenses against threats. Centralized IT benefits from leveraging economies of scale, particularly in technology solutions and services, which further efficiency and financial management.

§6.3.2 Risks and Pitfalls

Innovation in proposal development is driven by the PIs being agile for responding to the funding agency call. This requires PIs rapidly marshaling a team of innovative individuals that are also well versed in the subject matter, data, and possess the requisite cloud-native and computational skills around IT. Authority to prioritize duties and responsibilities of those individuals drives what proposals we can be responsive to. Centralizing IT roles and our IT staff may result in a reduced team agility and subject matter expertise, both of which are key components to be successful in being recommended for award.

The Organization Chart (Fig. 2) of campus IT is a key element during the proposal review process for many medium and large-scale projects. In the supplemental materials (§7.3), we provide several other large University IT department organizational charts for basic comparison. Demonstrating the PI and team can deliver on the vision requires management authority over many aspects of the staffing. The equivalent of outsourcing that to a different organization is detrimental in the eyes of proposal reviewers, and will hurt our competitiveness as many of the employees perform dual roles in the project.

Staff members are central to workforce development for projects as many of the IT centric staff oversee students and train researchers on analysis topics and tools. Many of these students and researchers then join other departments and units to enrich their capabilities. Losing this continuum of training and learning capabilities will severely restrict our experiential learning opportunities and specialized workforce development. For example, Development and Operations (DevOps) has become essential staffing for most cutting-edge research projects, where dual roles are highly blended and provided by one individual:

- DevOps: Software Development + IT Operations
- MLOps: Machine Learning + IT Operations

More importantly, centralized IT individuals not trained in close proximity to researchers that have holistically grown into these dual roles during the decentralized IT era will reduce our human resources capacity and lower our academic output of trained individuals ready to enter the workforce. Recent reports from small

decentralized IT units have found that they are effectively managed[107]. Centralization of IT for research teams is likely to have long-term consequences about whether and how we innovate.

§6.3.3 Mitigation and Alternative Approaches

Several other peer-group R1 universities rely on "Information Technology Advisory Councils (ITAC)"[108] which are responsible for guiding Information Technology (IT) decisions through their Offices of IT (OIT) or UITS equivalents.

Arizona State University has a clearly specified governance structure[109] which includes its IT Governance and Policy as well as Data Privacy and Data Governance. Both ASU's IT and Data Governance are supervised by Advisory Committees and Standards Working Groups. Similarly, the University of Utah's IT department relies on a group of IT Governance committees[110] which include its strategic vision and oversight.[111]

University of Utah's IT Governance structure[112] is as follows:

- The Architecture and New Technology Committee (ANTC) is entrusted with hearing IT issues and makes recommendations that affect IT architecture and architecture standards, IT common services, and the adoption and implementation of new technologies. Its recommendations go to the SITC. Both the SITC and ANTC may create ad hoc committees to address specific issues of strategic importance.
- Strategic Information Technology Committee (SITC) was formed to raise, hear, and discuss IT issues that affect significant portions of the University community or cross multiple areas of oversight. Its recommendations go to the University's executive leadership team for a final decision.
- Enterprise Web Advisory Council (EWAC) is an ad-hoc committee entrusted with raising, hearing and discussing issues that affect University web properties, its online ecosystem, and web visitors.
- University Geographical Information Services (UGIS) subcommittee is an ad-hoc committee convened by the ANTC.
- Teaching and Learning Portfolio (TLP) focuses on technology to support teaching and learning across campus.

Duke University recently commissioned a Research Support Needs Report[113] which recommended 12 changes to their IT governance strategy:

---

[107] https://www.azregents.edu/sites/default/files/reports/UA-Decentralized-Unit-%20IT-Genl-Cntrls-Review-Facilities-Mgt-Mar-2022.pdf
[108] https://itac.duke.edu/, https://www.colorado.edu/information-technology/it-governance, https://it.tamu.edu/about/it-governance/index.php
[109] https://tech.asu.edu/asu-it-governance, https://tech.asu.edu/sites/default/files/uto-it-governance-paper-2021.pdf
[110] https://it.utah.edu/cio/it-governance-overview.php
[111] https://it.utah.edu/cio/it-governance-committees/sitc-overview.php,
https://it.utah.edu/_resources/documents/cio/strategic_plans/fy24-27-uit-strategic-plan.pdf ,
https://it.utah.edu/_resources/documents/cio/strategic_plans/fy24-27-campus-strategic-plan.pdf
[112] https://it.utah.edu/cio/it-governance-overview.php
[113] https://itac.duke.edu/resource/research-it-needs/

- Additional Personnel: Proposed adding 15-20 full-time equivalents (FTEs) across their Libraries, the Office for Research and Innovation (ORI [UArizona RII Equivalent]), their Office of Information Technology (OIT [UITS equivalent]), and Schools to support new types of research and provide consistent offerings.

- Data Management Tools: devise tools to manage data for their entire lifecycle, develop a better understanding of cloud and on-premises storage costs, and clarify policies around data residency. Recommends providing storage capacity to meet the needs of 80% of active research projects.

- Storage Flexibility: Meet the differing storage needs for secure vs public access datasets that comply with regulations.

- Additional Virtual Machine (VM) Support: enhance the capability to provision VMs for the Duke Compute Cluster for researchers, postdocs and graduate stdudent's utilization.

- Secure and Protected Enclaves: Institute protected enclaves (HIPAA, CUI, ITAR, FERPA, RedCAP) to secure and encapsulate individual project data with the requisite security protections and mandates.

- Secure Compute Cluster Services: Calls for providing secure computing cluster services that are functionally equivalent to their existing VM and other offerings.

- Support for AI/ML Research: Capacity for AI/ML and other research through GPUs, similar to the DCC's on-demand CPU access.

- Risk-Based Security Approach: Advises using a risk-based approach to establish security and compliance expectations at a project level, including guidance for requesting exceptions.

- Cross-Department Virtual Teams: build cross-department support teams across Schools and in ORI, OIT, and Libraries.

- Self-Service Tool for Service Selection: Suggests developing a self-service tool to guide service selection based on data classification and access attributes.

- Faculty Startup Packages: provide computational cluster support for faculty startup packages, fund semi-autonomous sub-clusters.

- Development of Training Programs: Develop new training programs for faculty and students, ensure IT personnel are well-trained on research support services.

§6.4 Cloud

We strongly encourage UITS to continue its 'cloud-first' or the so-called 'cloud-native' approach to IT design for services and administration. Ensuring that the university administration is operating effectively and efficiently on the cloud is and should continue to be a top priority. We do however want to reemphasize that the adoption of cloud computing and commercial cloud providers across campus departments and for research computing is not a *zero-sum* or *all-or-nothing* decision.

UArizona has been a trailblazer in cloud integration for many years, and in many ways is the premier R1 university in the country utilizing cloud for its operations. This committee would like to recognize the foresight and the ongoing importance of transitioning the university's IT to a modern cloud infrastructure. UITS has been a leader in cloud innovation since before 2017[114] with multiple awards supporting cloud services for the national research community[115].

§6.4.1 Benefits and Opportunities

Being cloud-native and having open access to cloud services, high performance computing, and large data storage makes UArizona competitive for a range of research and development applications.

The 2022 "Nelson Memo"[116] and subsequent transmissions from the White House Office of Science and Technology Policy reinforce a new mandate that all federally funded research projects must publish their data upon publication, without embargo, and continue to service these scientific research data to the public beyond 2025[117].

§6.4.2 Risks and Pitfalls

Our most significant concern includes the potential for "vendor lock-in" with AWS, where we become dependent on a single cloud provider's services, leading to increased costs over time. This dependency can complicate migration to another cloud service provider. The variable cost models of cloud providers and services, particularly for data egress and specialized computing resources necessitates a robust understanding of management of cloud security practices to protect sensitive, private, and confidential, and controlled data. Complying with regulatory requirements is an additional challenge that requires continuous attention.

---

[114] https://it.arizona.edu/news/ua-wins-cloud-leadership-awards
[115] https://news.arizona.edu/story/cyverse-receives-third-nsf-award-enabling-data-science
[116] https://www.whitehouse.gov/ostp/news-updates/2022/08/25/ostp-issues-guidance-to-make-federally-funded-research-freely-available-without-delay
[117] https://www.whitehouse.gov/ostp/news-updates/2023/01/11/fact-sheet-biden-harris-administration-announces-new-actions-to-advance-open-and-equitable-research/, https://whitehouse.gov/ostp/news-updates/2024/01/31/fact-sheet-biden-harris-administration-marks-the-anniversary-of-ostps-year-of-open-science/

We are also concerned about moving academic departments teaching and research programs into the cloud. The cost and time to educate IT personnel at the department level will be high and take a significant amount of time. The burden of this transition, and the liability for the costs of the change are not well articulated in the IT centralization plan so far.

§6.4.3 Mitigation and Alternative Approaches

We recommend adopting a multi-cloud approach which prevents vendor lock-in, allowing UArizona to leverage the best services and pricing from multiple vendors, and thus increasing our bargaining power. Implementing strong governance policies and cloud management controls can help monitor cloud usage and costs, ensuring that university and research award budgets are adhered to, and UArizona avoids unexpected financial burdens.

Developing and providing digital and cloud literacy training for IT staff and researchers will also ensure the UArizona is well prepared for utilizing cloud resources safely and efficiently. Open-source tools and platforms should be considered wherever possible to enhance interoperability and data mobility across cloud environments.

Suggested mitigations to avoid vendor lock-in by:

- Developing multi-cloud evaluation metrics for costs which reveal changes in pricing,
- Keep data mobile - use open-source data formats, and off-site off-vendor backups,
- Reusable Application design - use composable templates using open source orchestration tools (e.g., Kubernetes & Terraform) which allow (re)deployment to other cloud providers,
- Reproducibility - containerize workflows and leverage Infrastructure as Code (IaC) for most applications and services.

Individuals and departments can work to get free access to commercial cloud providers. There are multiple opportunities for credits (free cloud computing and storage) on any of the three major cloud providers.

Commercial Cloud Credits for Research

- AWS Cloud Credit for Research
- Google Cloud Research Credits
- Microsoft Azure Research Credits

Commercial Cloud Credits for Education

- AWS Cloud for Education
- Google Cloud for Education
- Microsoft Azure for Education
    - GitHub Education (CodeSpaces)

Open Source Clouds

OpenStack is the most widely deployed open source cloud software in the world, there are publicly available OpenStack clouds which are available to UArizona faculty and students:

Public OpenStack Clouds

- JetStream2 - US NSF funded OpenStack Cloud for research and education. UArizona researchers are a subaward and are developing one of Jetstream2's featured user interfaces.
- CyVerse (UArizona) Cloud - CyVerse operates OpenStack Clouds from the Co-location space at the research computing center

§6.5 Research Computing

Mandates that researchers transition to commercial cloud for high performance computing (HPC), data intensive scientific research particularly for GPU/TPU-based computing, e.g. Artificial Intelligence (AI) and Machine Learning (ML) and for research data storage and hosting is not recommended and is strongly advised against. The financial cost to operate the University's research enterprise on commercial cloud could balloon the expenses, resulting in a loss of competitiveness on future extramural research proposals/awards.

Recently at the January 18th, 2024 NSF CI-Compass[118] meeting in Long Beach CA, Dan Stanzione PhD the Executive Director of the Texas Advanced Computing Center (TACC)[119], home to the next leadership class computing center for the NSF gave the following anecdote during a panel talk "What I wish I knew then,"

> *"... This came up this morning, but I mentioned it in the Q and A. Cloud prices have effectively tripled and more than that for AI. I used to price what we delivered [at TACC]. I did an analysis in 2020 where I*

[118] https://ci-compass.org/

[119] https://tacc.utexas.edu/about/staff-directory/dan-stanzione/

figured just the compute time on CPUs that we put out [at TACC] was worth about $120 million of Amazon [AWS] time per year. I did it again in December and it came out to $418 million.

We [at TACC] do about the same and we're spending $35 to $40 million [per year] to deliver that, including people. So it's sort of 11:1 [return on investment], and that assumes that all storage in the cloud is free and all networking in the cloud is free and that there's no people costs associated with going to the cloud. If you believe all those things are true, then it's only 11:1, per year.

[audience inaudible] Yeah, we delivered $418 million of, oh, and I left out all the GPUs because the GPUs are astronomical.

[audience inaudible] Right. It would have been a billion dollars. Yeah, $418 million just in hours of CPUs delivered."

The take-aways of what Dr. Stanzione has said are: the value of on-premises research computing far exceeds developing or building similar solutions on commercial cloud providers. Consequences of a forced move in research computing onto commercial cloud providers could result in UArizona research costs increasing up to an order of magnitude.

§6.5.1 Benefits and Opportunities

Currently, Research Computing account holders fully utilize UArizona's HPC capacity. Therefore, Research Computing is meeting and exceeding the necessary cost-benefit ratio of justifying running computing on-premises versus on a commercial cloud provider. By owning and maintaining a HPC center, UITS generates massive cost-savings to UArizona and Sponsored Projects that rely upon this resource. Research Computing currently provides the faculty and staff with an equivalent value of $16,500,000 per annum relative to similar CPU resources on AWS[120].

For specific information and use-cases commercial cloud offers the ideal solutions for managing data and meeting the university security requirements. We recommend commercial cloud as-needed for sensitive, secure, and sovereign (CUI, ITAR, HIPAA, etc) data which are managed by university researchers, particularly in use-cases where data are funded by federal government and multi-institutional collaborative research efforts.

New federal and state funding mandates are intended to meet the challenges of the new AI revolution. Billions of dollars of research are now flowing into AI related acquisitions of hardware and software development. Investment into new on-premises HPC resources should include GPUs to help manage private and self-hosted AI research and LLM deployments which can ensure data privacy and security.

[120] https://it.arizona.edu/news/high-performance-computing-research, assuming 27.5M cpu hours per month for $1,375,000 per month on average over last 12 months.

An important component of AI research is well structured, machine readable data. Unique datasets which are proprietary or owned by the UArizona or ABOR have value to AI training. By maintaining the authority to control private, sensitive, secure, and sovereign datasets, UArizona can create value in its public and private data commons.

§6.5.2 Risks and Pitfalls

We strongly advise that Faculty Senate to advocate to the Office of the CIO against migration of HPC into a commercial cloud computing contract for the following reasons:

> **Risk 1:** Many recent cost-benefit analyses have shown that commercial cloud costs are 4x to 10x more expensive over their lifetime than on-premises computing.[121]
>
> **Risk 2:** Numerous companies and institutions who previously moved to commercial cloud are now migrating back to on-premises computing and data storage in order to save money.[122]
>
> **Risk 3:** There are numerous reports of cloud computing costs growing unexpectedly over time[123] which have negatively impacted projects with fixed budgets.[124]

Major research projects all operate on-premises for very specific, financially grounded, reasons: the cost to run large research operations on commercial cloud, at the scale of modern research, is financially prohibitive. Researchers operate on very tight research budgets, which are calculated years in advance. If commercial cloud providers were offering cheaper services than what is possible with on-premises services, these projects would have already migrated.

§6.5.3 Mitigation and Alternative Approaches

The January 2024 NSF Major Facilities Cloud Use Cases and Considerations report highlights the cost considerations, navigating vendor lock-in, and managing the economics of cloud platforms for research computing in depth. For more information, we recommend that interested parties read that report here: https://doi.org/10.5281/zenodo.10481410.

---

[121] https://dl.acm.org/doi/10.1145/3311790.3396642, https://doi.org/10.1145/3491418.3535131, https://dl.acm.org/doi/10.1145/3332186.3332228, https://doi.org/10.1145/3355738.3355749

[122] https://www.forbes.com/sites/peterbendorsamuel/2021/08/10/why-is-cloud-migration-reversing-from-public-to-on-premises-private-clouds/, https://world.hey.com/dhh/why-we-re-leaving-the-cloud-654b47e0, https://dev.37signals.com/our-cloud-spend-in-2022, https://world.hey.com/dhh/the-big-cloud-exit-faq-20274010, https://drive.google.com/file/d/1zVwTw2_cjbfeoDw7dWHRrqLNBj2w7eSA/view?usp=drive_link

[123] https://www.wsj.com/articles/cios-still-waiting-for-cloud-investments-to-pay-off-11664449203

[124] https://world.hey.com/dhh/the-big-cloud-exit-faq-20274010

Future investment into the 2025 HPC refresh will help alleviate and improve conditions for research computing users. NSF has several opportunities to bring additional research dollars into a new infrastructure acquisition[125] which are currently being pursued.

Investment from private donors or corporations is another area where new infrastructure resources may be acquired. Companies like NVIDIA have supported University partnerships and acquisitions of HPC and AI data centers with their GPU hardware[126].

§6.6 Human Resources (Education & professional development)

The development of human resources around the use of modern cloud-based research cyberinfrastructure is one of UArizona's greatest and most unsung capabilities. New degrees in software engineering in the College of Engineering[127] and data science as a bachelors[128], masters[129], and certificates are appearing across many colleges and schools. The College of Applied Sciences and Technology (CAST)[130] specializes in innovative, online programs that prepare students for the most in-demand 21st-century jobs around cybersecurity and defense.

Modern cyberinfrastructure includes three interoperating components: hardware, software, and people.

- Software - drives efficiency and improves over time
    - Infrastructure as Code
    - Continuous frameworks
    - Free and Open Source Software (FOSS)
- Hardware - scalable and elastic, depreciates rapidly and requires maintenance
    - High Speed Networks - Internet2 & Sun Corridor
    - Scalable Computing
    - Security
- People – manage and innovate, and maintain systems
    - IT professionals
    - Researchers
    - Cybersecurity Teams

People are the most often overlooked component of IT and the cyberinfrastructure ecosystem around it. The role of the university is to train and develop new professionals and prepare them for current market employment

[125] https://new.nsf.gov/funding/opportunities/mid-scale-research-infrastructure-2-mid-scale-ri-2
[126] https://news.ufl.edu/2020/07/nvidia-partnership/
[127] https://www.arizona.edu/degree-search/majors/software-engineering
[128] https://www.arizona.edu/degree-search/majors/statistics-and-data-science-bs
[129] https://ischool.arizona.edu/ms-data-science
[130] https://informatics.azcast.arizona.edu/

opportunities. UArizona is deeply invested in the education and professional development of cyberinfrastructure and cybersecurity specialists, software engineers, software developers, cloud architects, AI researchers, data scientists, and research software engineers.

§6.6.1 Benefits and Opportunities

UArizona is leading the professional development of the next generation of data science, cloud, and cyberinfrastructure professionals through departments like the iSchool and CAST. Maintaining competitiveness in a rapidly evolving landscape of AI, cloud, and data driven research is critical to the future of UArizona. New degrees and certification programs in software engineering, data science, and related fields across various colleges underscores UArizona's commitment to aligning educational offerings with the demands of a modern workforce.

UArizona supported projects which rely on UITS cyberinfrastructure include CyVerse, which has employed over 100 students and postdoctoral researchers over the last 15 years. CyVerse has employed an additional 99 staff members, many of whom have left for industry and commercial cloud-based jobs.

UArizona supports unique capabilities and skills related to the development of modern IT, research science, cloud computing, and data management which were highlighted as part of the White House's 2023 Year of Open Science[131] and are important components of UArizona's future research eligibility for federal research awards.

§6.6.2 Risks and Pitfalls

Reduction in force and loss of state support may slow or end efforts to redesign curriculum around 4th Industrial Revolution based careers. Loss of support could severely impact UArizona's ability to maintain and expand its educational programs around IT, cloud, cyberinfrastructure and cybersecurity.

Cuts to funding risk the investment into faculty development and innovation in the rapidly evolving technology space. These may reduce our reputation as leaders in cyberinfrastructure and cybersecurity research and education.

§6.6.3 Mitigation and Alternative Approaches

Strategic investment has helped to create CAST and other programs in cyberinfrastructure and data science. Continuing to support 21st century workforce jobs around AI, cybersecurity, and cloud IT will be critical to keeping UArizona ahead of its peers in cyberspace.

---

131 https://www.whitehouse.gov/ostp/news-updates/2024/01/31/fact-sheet-biden-harris-administration-marks-the-anniversary-of-ostps-year-of-open-science

Partnerships with industry and government can provide alternative funding sources and opportunities for curriculum development ensuring that programs remain cutting edge.

§7 Appendices and Supporting Materials

§7.1 Facilities

The HPC clusters and storage are housed in the 1,800 sq ft Research Data Center (RDC), a state-of-the-art computer storage facility that triples the university's previous capacity to host centralized large computer clusters. The RDC offers an uninterruptible power supply that includes 400 kVA power consumption for HPC clusters and storage systems, and 1,600 kVA available backup generator power for RDC. The RDC has a 70 ton AC cooling capacity along with a chilled water supply to support 20 racks.

UA HPC systems have a centrally purchased "core" which is available for all UA researchers under fair-share allocations for each of the HPC system 100,000 cpu-wall hours per month per principal investigator (PI). Beyond the normal allocation users can submit "windfall" jobs that use otherwise idle cycles. UA Research groups that require more than the fair-share use can "buy-in", providing funding for nodes to be added to the existing systems and receiving high priority allocations proportional to the cycles added by the funded nodes. Buy-in includes data center space, redundant power (utility, UPS, generator), cooling (water cooled racks), network connections, and system administration at no additional charge.

Faculty access to UA High Performance Computing equipment includes:

- **Puma (2020)**: This system has 320 nodes with dual 48-core AMD EPYC 7642 for a total of 30,000 CPU cores. Each node has either 512GB or 3TB of RAM for a total memory of 176TB. The system also has 60 NVIDIA V100 GPUs. Interconnects are 25Gb Ethernet and the system runs CentOS 7 and supports Distributed, Serial (High Throughput Computing), and GPU computation.

- **Ocelote (2017)**: Lenovo NeXtScale nx360 M5. This system has 422 nodes with dual 14-core Xeon Haswell E5-2695 for a total of 11,752 CPU cores. Each node has either 192GB or 2TB of RAM for a total memory of 83TB. The system also has 46 NVIDIA P100. Interconnects are FDR Infiniband and the system runs CentOS 7 and supports MPI, Parallel, OpenMP, Serial, and GPU computation.

- **El Gato (2013)**: IBM System x iDataPlex dx360 M4. This system has 131 nodes with Dual 8-core Xeon Ivy Bridge E5-2650 for a total of 2160 CPU cores. Each node has either 64 or 256GB of RAM for a total memory of 26TB. The system was provisioned with 137 NVIDIA K20x GPUs which have reached end of life and are no longer available to researchers. Interconnects are FDR Infiniband and the

system runs CentOS 7 and supports distributed and serial computation. El Gato is intended to be retired with the acquisition of the next HPC cluster.

All HPC clusters are mounted to an all-flash high performance disk array so that user data is accessible from any of the computing systems. This expandable array has over 2PB of available storage and there is no charge for usage as it is centrally funded with the compute clusters. An additional array is available in the RDC with 1.5PB of capacity for longer term project or campaign data. This array is available for rental at a subsidized rate of $47.50 per TB per year.

For archival data, an AWS backed service is available with the first 1TB subsidized by UITS. Recently, a third data management and storage service, Research Desktop Attached Storage (R-DAS) has been made available and provides up to 5TB of free storage to each faculty researcher.

In the RDC, CyVerse manages 11 PB of storage using the open-source iRODS data management platform. CyVerse is geographically distributed, with a full back-up off-site mirror at TACC. A production Kubernetes cluster with 1,052 cpu cores, 21 GPUs, 7.68TB of RAM, and 191TB of local storage. The cloud infrastructure (OpenStack) contains 1,192 cores with 16TB of RAM and 428TB Ceph Storage. A condor pool (612 cores) provides access for rapid turnaround tasks. A modest dedicated virtualization cluster (224 cores) is primarily utilized for persistent hosting of web applications and databases.

- **Networking:** The UArizona also partners with ASU and NAU on the Sun Corridor Network.[132] The current connection from UArizona to Sun Corridor is dual 10G, while Sun Corridor is connected to Internet2[133] via dual 100G connections in Tucson and Phoenix. The UArizona's Research Data Center has 40GB/s connections to the UArizona core with all the servers connected by 1GB/s or 10GB/s connections.

Real-world tests of UA's parallel data transfer system can move ~1TB of data in ~5 hours between research institutions located in different states (UC Berkeley to UArizona).

In addition to direct connectivity to the campus network at the building level, researchers have an opportunity to use a Science DMZ for fast and high volume data transfers to outside collaborating institutions, using National LambdaRail or Internet2, as examples.

The Science DMZ is deployed at the UArizona network perimeter, outside border firewalls, and is directly connected to Sun Corridor via 10G link. It is secured via static access lists deployed at the Sun Corridor router without impact to performance.

[132] https://suncorridor.org/
[133] https://internet2.edu/

There are two high-performance Data Transfer Nodes (DTNs) deployed in the Science DMZ. DTN's are dedicated servers with hardware and operating system optimized for high speed transfer.

§7.2 Budgets

Table 3: Central IT and Campus IT expenditures from UITS annual financial reports (Table 5 below). n/a are used for specific values which could not be found in the available annual financial reports. FY2023 is not available

Fiscal Year	2017	2018[134]	2019[135]	2020[136]	2021[137]	2022[138]	2023
Managed Cloud Services	n/a	n/a	$1,784,000	n/a	$2,843,019	$4,141,593	n/a
Personnel (salary/wage)	n/a	n/a	$22,054,376	$24,327,625	$22,209,683	$23,796,123	n/a
Central IT Expenditures	$56,809,063	$62,905,197	$62,900,000	$77,665,450	$62,286,289	$69,274,869	n/a
Campus IT Expenditures	$58,364,883	$66,700,000	$66,700,000	n/a	n/a	n/a	n/a
Total IT Expenditures	$117,113,946	$129,605,197	$129,600,000	$128,100,000	$130,500,000	$140,984,824	n/a

Table 4: Equipment End of Life (EOL), replacement costs, and total network expenditures by year. In UITS Yearly reports the presentation of EOL (total, network, and classroom), replacement cost for the network, and expenses are reported differently or not reported.

	FY2018	FY2019	FY2020	FY2021	FY2022	FY2023
EOL Network				$12,400,000	$5,500,000	n/a
EOL Classroom				$2,900,000	$4,100,000	n/a
EOL total	$5,000,000	$8,800,000	$7,800,000			n/a
Replacement Cost	$23,000,000	$29,000,000	$29,000,000			n/a

[134] https://arizona.app.box.com/v/UITS-Annual-Report-FY2018
[135] https://arizona.app.box.com/v/CIO-Annual-Report-FY2019
[136] https://arizona.app.box.com/v/IT-Annual-Report-FY2020
[137] https://live-azs-it-annualreport.pantheonsite.io/sites/default/files/2022-04/UArizona_IT_AnnualReport_FY2021_0.pdf
[138] https://live-azs-it-annualreport.pantheonsite.io/sites/default/files/2023-08/IT_AnnualReport_2022.pdf

Network Infrastructure Expenses			$5,187,764	$8,209,242	$10,708,037	n/a

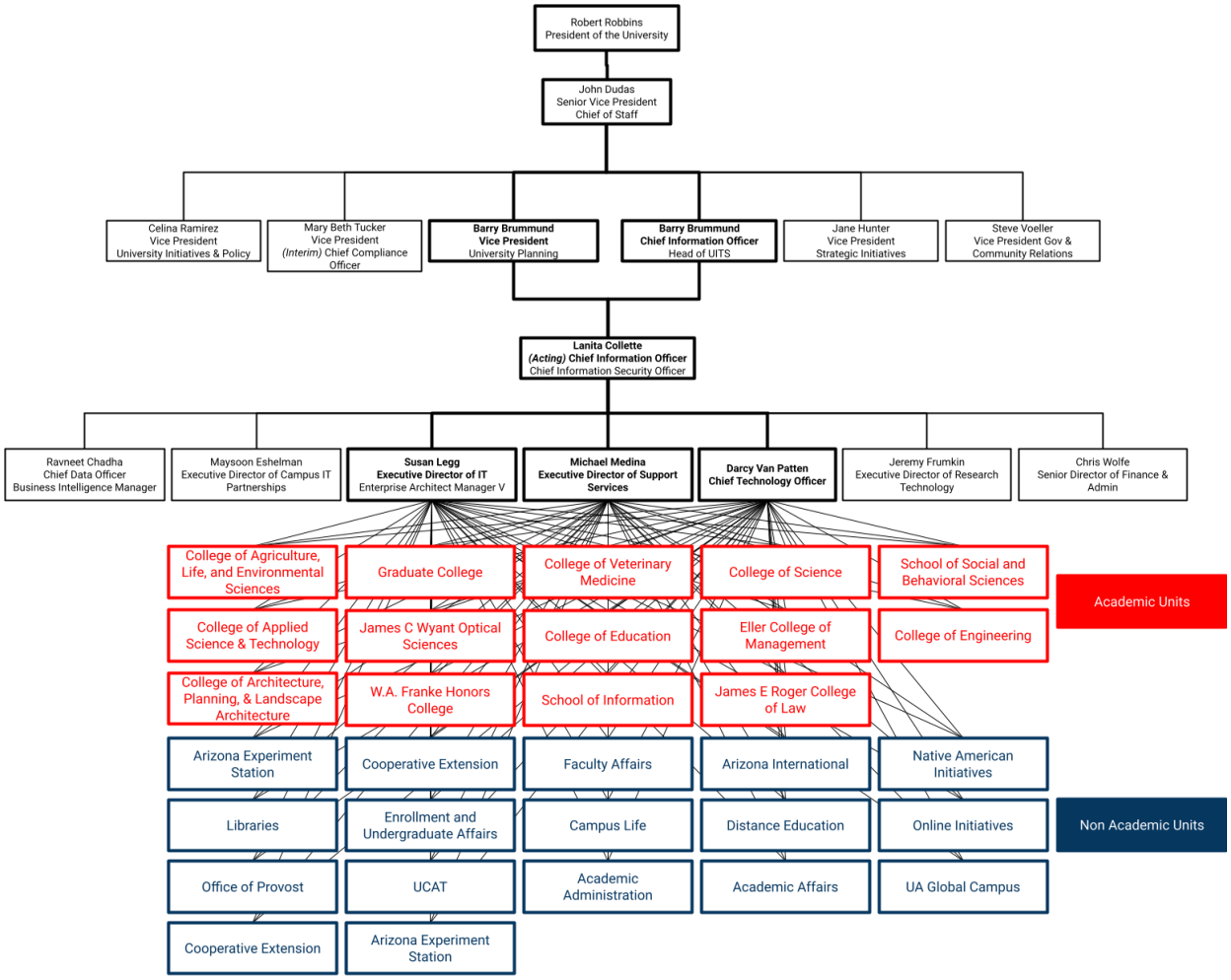
Table 5: UITS Annual Reporting, Main Campus Appropriation Budgets, UA Operating Budgets, and Arizona Appropriations Budgets from 2013 until 2023, all files are on publicly accessible websites.

FY	UITS Annual Reports (w/ some budget)	Main Campus Appropriation Budgets	UArizona Financial Reports	UA Operating Budget
2013	https://web.archive.org/web/20160101193229/http://cio.arizona.edu/sites/cio/files/14/03/cio-annual-report-2013.pdf	https://www.azjlbc.gov/13AR/uniumain.pdf	https://financialservices.arizona.edu/sites/default/files/2021-06/afr2013.pdf	n/a
2014	https://web.archive.org/web/20150221075730/http://cio.arizona.edu/sites/cio/files/14/11/cio-annual-report-2014.pdf	https://www.azjlbc.gov/14AR/uniumain.pdf	https://financialservices.arizona.edu/sites/default/files/2021-06/afr2014.pdf	
2015	n/a	https://www.azjlbc.gov/15AR/uniumain.pdf	https://financialservices.arizona.edu/sites/default/files/2021-06/afr2015.pdf	
2016	n/a	https://www.azjlbc.gov/16AR/uniumain.pdf	https://financialservices.arizona.edu/sites/default/files/2021-06/afr2016.pdf	
2017	n/a	https://www.azjlbc.gov/17AR/uniumain.pdf	https://financialservices.arizona.edu/sites/default/files/2021-06/afr2017.pdf	
2018	https://arizona.app.box.com/v/UITS-Annual-Report-FY2018	https://www.azjlbc.gov/18AR/uniumain.pdf	https://financialservices.arizona.edu/sites/default/files/2021-06/afr2018.pdf	
2019	https://arizona.app.box.com/v/CIO-Annual-Report-FY2019	https://www.azjlbc.gov/19AR/uniumain.pdf	https://financialservices.arizona.edu/sites/default/files/2021-06/afr2019.pdf	
2020	https://arizona.app.box.com/v/IT-Annual-Report-FY2020	https://www.azjlbc.gov/20AR/uniumain.pdf	https://financialservices.arizona.edu/sites/default/files/2021-06/afr2020.pdf	
2021	https://live-azs-it-annualreport.pantheonsite.io/sites/default/files/20	https://www.azjlbc.gov/21AR/uniumain.pdf	https://financialservices.arizona.edu/sites/default/files/2021-11/acfr2021.pdf	https://azmemory.azlibrary.gov/nodes/view/93104

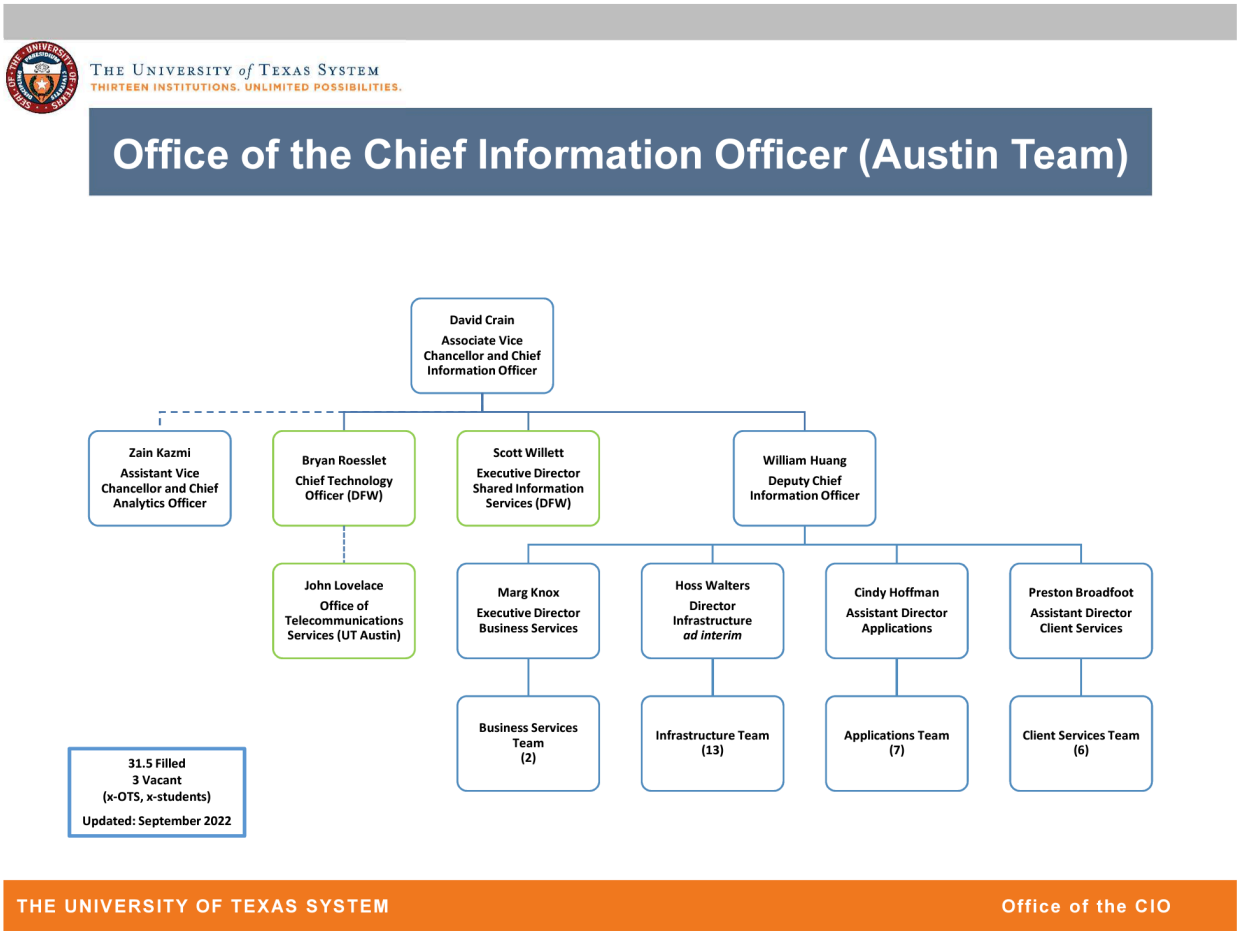
	22-04/UArizona_IT_AnnualReport_FY2021_0.pdf			
2022	http://live-azs-it-annualreport.pantheonsite.io/sites/default/files/2023-08/IT_AnnualReport_2022.pdf	https://www.azjlbc.gov/22AR/uniumain.pdf	https://financialservices.arizona.edu/sites/default/files/2022-10/acfr2022.pdf	https://repository.arizona.edu/handle/10150/670922
2023	n/a	https://www.azjlbc.gov/23AR/uniumain.pdf	https://financialservices.arizona.edu/sites/default/files/2023-10/acfr2023web.pdf	https://repository.arizona.edu/bitstream/handle/10150/670915/State_Operating_Budget_Book_FY23.pdf
2024	n/a	https://www.azjlbc.gov/24AR/uniumain.pdf	n/a	n/a

§7.3 Example Organizational Charts from Peer Institutions

For reference, the current [presumed] UArizona Organizational Chart

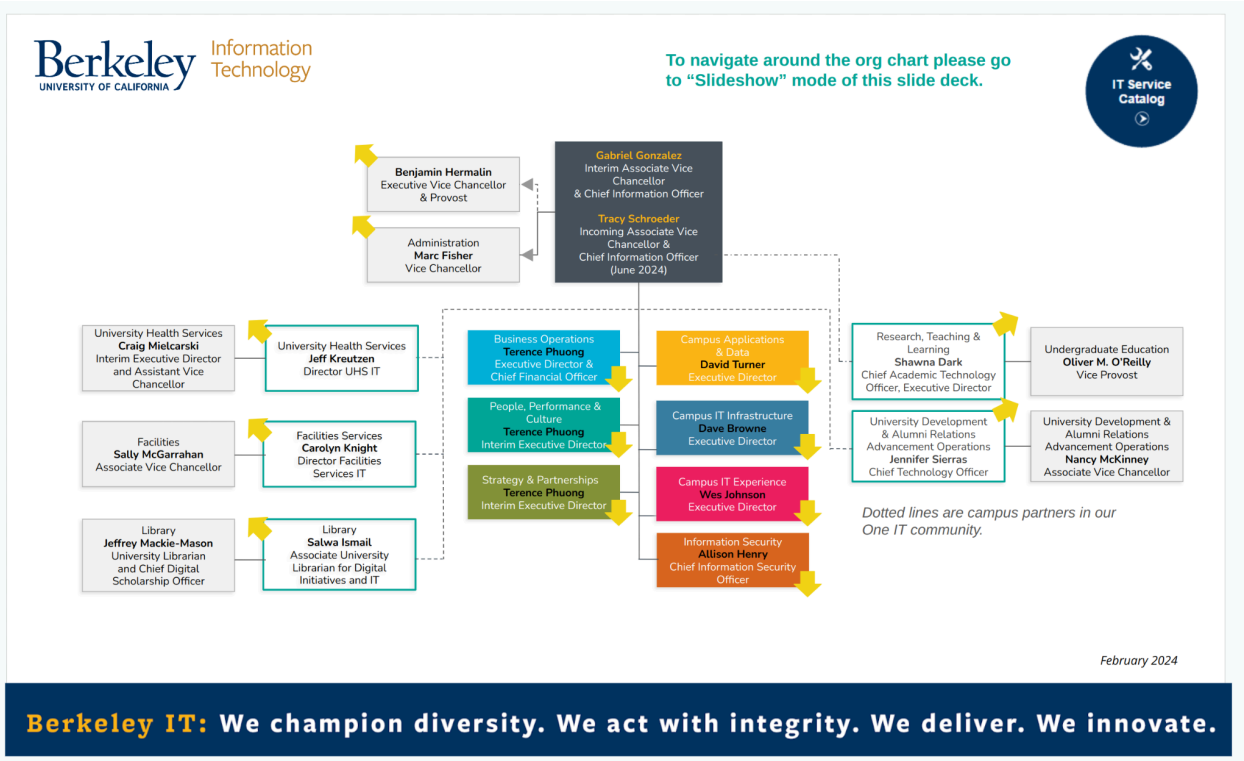


University of Texas (Austin)



[UT Austin CIO Office Organizational Chart]

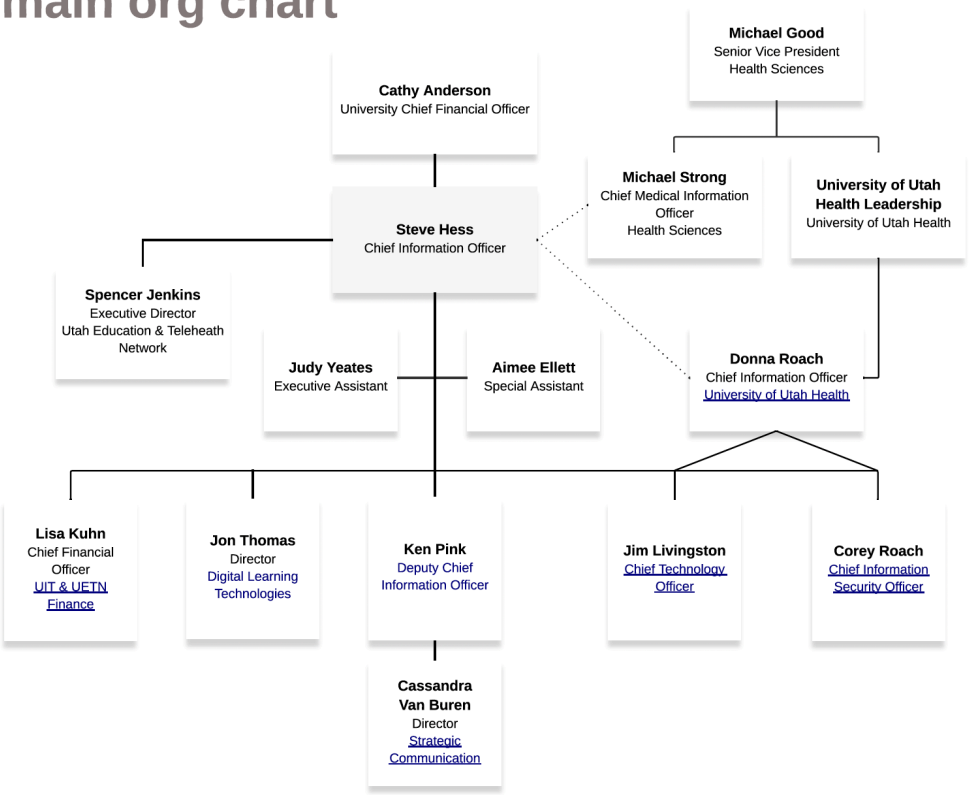
University of California Berkeley



[UC Berkeley Organizational Chart]

University of Utah

UIT main org chart

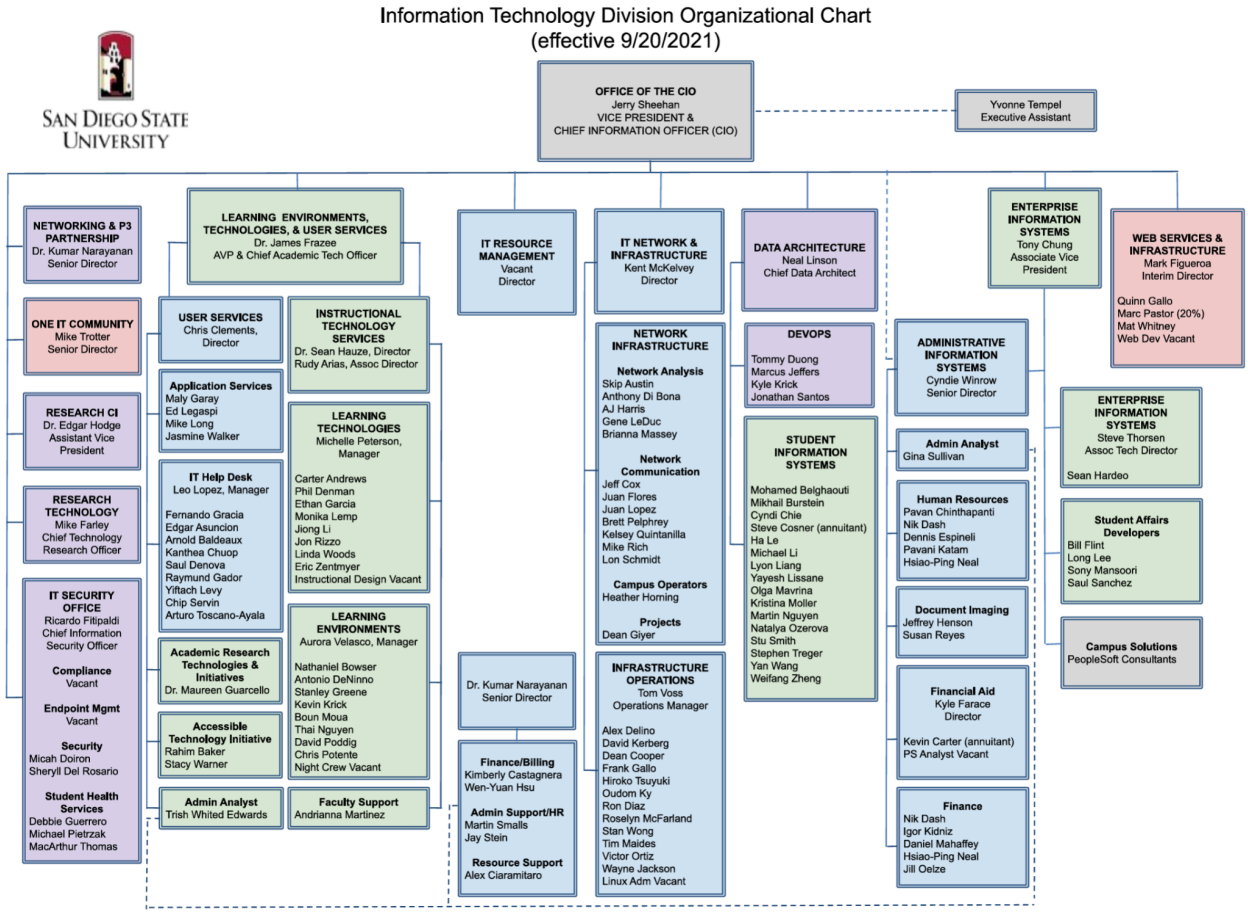


INFORMATION TECHNOLOGY
THE UNIVERSITY OF UTAH

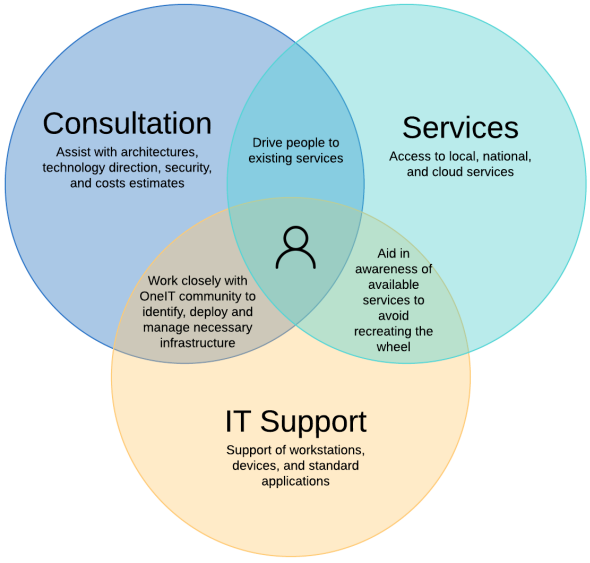
Updated 9/18/2023

https://it.utah.edu/orgcharts/index.php

San Diego State University

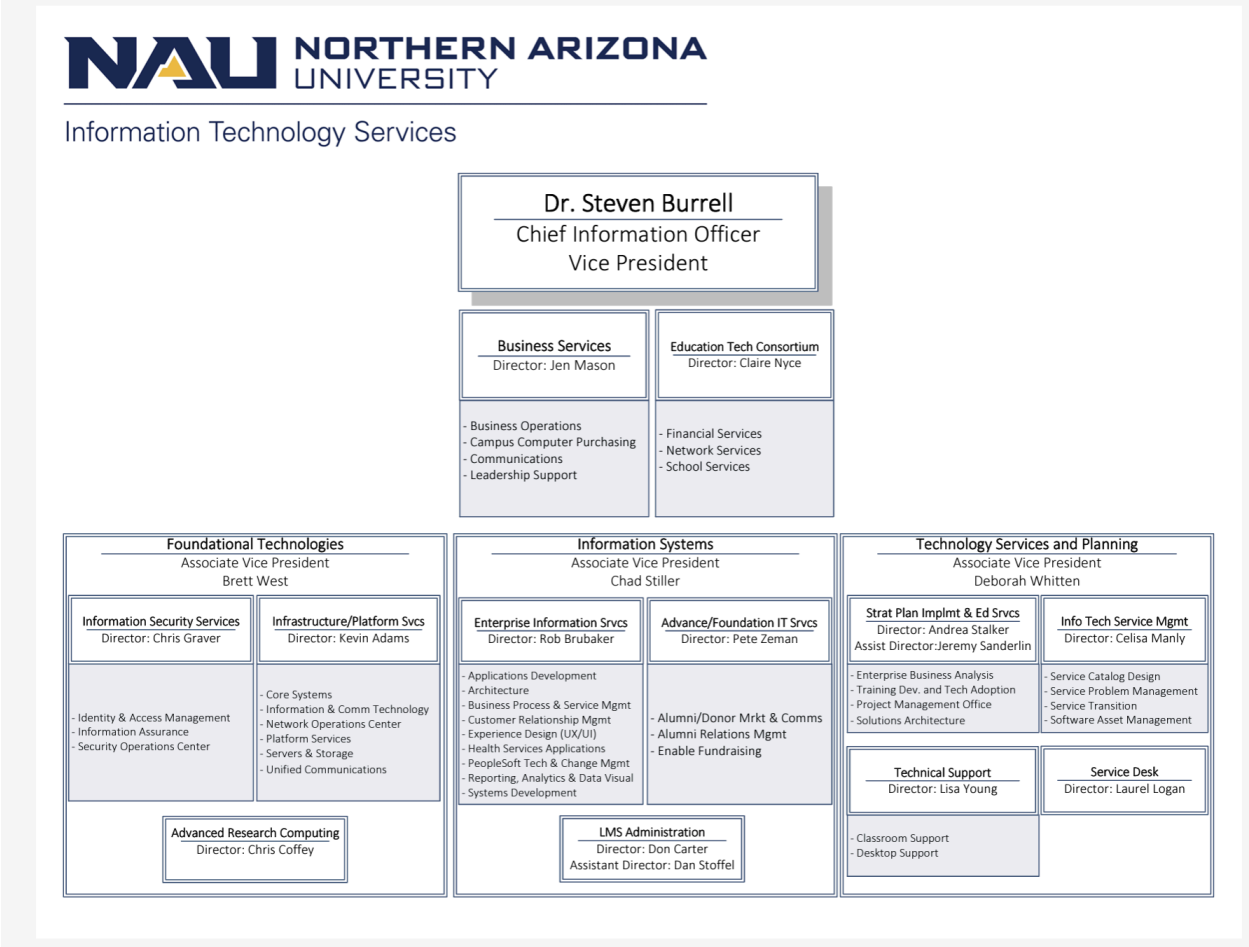


SDSU IT Organizational Chart



SDSU Consultation

Northern Arizona University



https://in.nau.edu/wp-content/uploads/sites/162/2024/01/ITS_Overall_Org_Chart.pdf