Digital Enablement: Powering the NC State Mission

The NC State 2030 IT Strategic Plan

FINAL - April 18, 2023

Overview

A review and refresh of the IT Strategic Plan was launched in the fall of 2022 to align with the new university strategic plan: **Wolfpack 2030: Powering the Extraordinary**. As part of the 2022 IT Community Event, we used a survey process and hosted an ideation session to gather input to update the IT Strategic Plan.

To accomplish updating the plan, we used three phases:

- Phase 1: Gathered input on updates and new IT goals via a survey, and then ranked the potential goals through a follow-up survey.
- Phase 2: Hosted an IT Community Event session to generate new strategies for the top-ranked themes and goals that emerged from the Phase 1 survey.
- Phase 3: Shared the outcomes from Phases 1 and 2 with the governance groups and worked to finalize the new strategic plan with additional input, discussion, and final agreement.

IT Strategic Goals

The process created five Goals and connected strategies for each goal. Below are the opportunities to improve IT across campus in support of the university's mission.

GOAL: Deliver world-class services and capabilities to NC State Faculty, Staff, and Students.

The NC State Wolfpack 2030 Strategic Plan has digital transformation embedded throughout the goals, strategies, and implementation. It is incumbent on university IT to ensure technology support and services are capable of enabling preeminence in research, scholarship, innovation, and collaboration by meeting the diverse IT needs of the community. Collectively, the IT community needs to develop processes and services that support the enterprise IT needs and also enable researchers, scholars, educators, staff, and students to gather, store, analyze, and share data in collaboration with people inside and outside the university.

Strategies:

- ## Perform a gap assessment of IT services across the university to achieve collaboration and improvements

  We need to review what IT services are available and missing across campus to meet the university requirements. To do that, we also need to look at what other R1 schools are doing. We have faculty asking how to do what they did at their previous schools. We want our services to be an incentive for faculty to come to NC State. We need to find out what faculty and staff need and determine where we aren't meeting those needs. We also need to think about whether the services we are providing meet what our customers want to do. Finally, we need to prioritize our services and actively determine which services to enhance and how to stop less valuable services.

  Before performing a survey or needs assessment that involves external partners and customers, we need to make sure that we are using terms that we all agree on and are understandable to customers. Finally, we need to make sure that we confirm our understanding so that we gather the right data.

- ## Create a university-wide services strategy/model

  As our IT organization matures its delivery and service functions, we need to formalize and standardize our service delivery and support models. This includes the alignment of services needed using our internal IT capabilities (Service Design/Org Design). A clearly defined model following ITIL will further support and empower the Research Facilitation Service (RFS) with automated delivery capabilities. It will also allow for the establishment of service (RFS) packages with clearly defined cost and service level commitments.

  To do this, we as IT service providers need to answer questions like who are our customers? What services and support do they want? Do we have the right groups and departments providing the right services and support to meet their needs? We need to make a clear differentiation between offering the function and/or service and how the customer who needs that capability can accomplish their goals. Customer service should be a guiding star.

  When defining services, we need to balance the large-scale, enterprise-level services and tools that are used by the majority of stakeholders with the bespoke needs of individual units. There are often common groupings where an enterprise solution can meet the needs of both.

To accomplish this, IT must first fully define the problem before deciding on a proposed solution or tool:

- **Capability:** The ability of our organization, person, process, application, IT service, or other configuration items to carry out an activity.
  - Example: Focused website to convey specific, helpful information to research participant or research team
- **Function:** an organizational entity, typically characterized by a special area of knowledge or experience.
  - Example: Install and manage servers and software to enable websites
- **Service:** A means of delivering value to our customers by facilitating outcomes that customers want to achieve without the customer having to manage specific costs and risks.
  - Example: Build and support a website for a specific project.

- **Empower students, faculty, and staff with access and training on the use and adoption of new technology**

  As part of this empowerment, we need to improve training, access and availability to a baseline of common technology. Training for activities directly related to security and safety risk is required. We should consider expanding these types of training as well as their delivery models.

  Peer-to-peer support and influencer models are critical for success of adoption of new solutions. Part of that influencer model includes the university leadership. These training activities need to be available to faculty, staff, and students. Requirements that vary by role, responsibility, or allow access should be included.

GOAL: Foster an environment of belonging, collaboration, and connectedness for IT-focused staff to strengthen culture and innovation.

IT Governance needs to help develop an IT workforce plan that supports university goals to attract, develop and retain talent. Our people are our most valuable asset in driving transformational change. We need to create a community of inclusive excellence that empowers team members to do their best work which will help drive institutional effectiveness. Being collaborative and transparent using enhanced governance-driven decision-making and prioritizing human and technical resources will result in the most impactful strategy-oriented initiatives and projects.

Strategies:

- **Clearly define the expected behaviors that support our people and ensure they feel appreciated and are successful.**

  Recognizing that our people need to feel appreciated and heard to feel included and part of the group is critical. Until we address this fundamental human aspect, we cannot be successful. A strong sense of accomplishment goes a long way to retaining people. How do we develop a culture where management can execute and emulate that agreed-upon and supported culture?

  Developing a key set of cultural attributes that we all know, embrace, and support will go a long way to helping improve culture. This could be as simple as acknowledging the values in the university strategic plan or incorporating the IT Guiding Principles from the previous IT Strategic Plan.

- **Develop activities, approaches, and tools to help people build the community we all desire.**

  There are various opportunities and activities to learn, participate and embrace approaches to build a strong community and culture. As a university, we have an even greater number of opportunities to participate and even help lead such activities. It is important that we understand people need multiple ways to become connected.

  There are many many well-known group activities that help people explore differences and commonalities. We should work to expose our entire community to different tools and ideas that promote team success and collaboration acknowledging our current hybrid work environment. We must provide tools and support to make this hybrid culture successful where all employees have a sense of belonging.

  Finally, ensure all managers and directors are expected to improve their leadership skills and embrace the inclusion of their team in providing input and guidance in decision-making. It should be the expectation that IT leaders are good managers and continually mentor their staff.

- **Ensure collaboration across the university to support diverse approaches, shared solutions, and community.**

As the university grows and budgets get stretched, we need to create a “collaboration first” mindset that we need for the future. To ensure we are all working together to create comprehensive shared solutions rather than single-point solutions to meet business needs, we must:

- Encourage shared and common solutions.
- Continue the development of structures and groups and the sharing of communications about efforts across units.
- Promote available affinity groups as ways to unify shared practices
- Continue to support and encourage participation in our IT Community events.
- Continuously improve IT Governance structures and campus-wide policies
- Listen to the customer voices

- **Provide career advancement pathways across the university to foster professional development and personal growth for IT personnel.**

We recognize that our employees are our most valuable resource and we must provide pathways for providing the ability to grow within our organization with opportunities for people to learn new skills and capabilities which will help reduce attrition. An example of possible actions could include:

- Emphasize workforce development and grow the people we want and need.
- Integrate internship programs across IT efforts.
- Support attracting diverse talent and people in IT employment
- Encourage innovation and exploration with the goal of common improvements
- Develop and support skill development activities and options for IT employees.
- Enable a program of mentors and networking opportunities for all IT employees

- **Pursue shared IT positions to support fractional demand across all units.**

IT experts often have unique and very specialized skills. These skills are often in demand but for limited time and projects with units across the university. Sharing a high-skill and high-salary position across departments can provide both in-demand skills and funding levels that match the needs. We will need to develop best practices to ensure success.

- Develop a shared marketplace for short-term projects where all units can contribute, fund or trade for a skill to support a project.
- Assess our university wide IT talent and build a skill/talent inventory.
- Create a process to allow short-term sharing of talent and best practice details on the management and oversight of how these shared resources will be reviewed and assessed.

GOAL: Ensure the security of digital assets through strong cybersecurity for all

Create a culture of cybersecurity and digital asset management to support the university's mission and to help the campus community protect itself. Securing the environment will help protect our students, research partners, faculty, and staff while helping to maintain and strengthen the university's reputation.

Strategies:

- ## Increase bi-directional university-wide engagement

  Cybersecurity is an organization-wide responsibility. Like any type of security, it can not be accomplished by a single top-down entity or only a grassroots approach. All parties must be involved, take appropriate responsibility, and help protect the whole. The campus vice chancellor for information technology and chief information officer (VCIT and CIO) is designated as the responsible cybersecurity person for campus. As a result, OIT has oversight responsibility for the university and cybersecurity activities. The campus chief information security officer (CISO) is delegated to be the lead for these activities. Security & Compliance uses a distributed model approach for these activities by working with campus governance, the Campus IT Directors (CITD), the Cybersecurity Liaison Program, and the Cybersecurity Awareness Team (CSAT). In turn, all campus personnel are responsible for implementing, supporting, and promoting the campus policies, rules, regulations, and standards to protect the campus IT infrastructure and data. This distributed and multi-level structure encourages bi-directional sharing, implementation, support and education.

- ## Leverage IT risk management to support university strategic initiatives

  The university Enterprise Risk Management (ERM) program identifies the top risks facing the university. The IT Risk Management program then takes the ERM IT risk and organizes it into its smaller risk components that can be addressed and implemented. These risk components should be addressed by policies and standards that need to be implemented across university divisions, colleges, and departments.

  Risk management also identifies the need to include cybersecurity in the early planning stages of initiatives, projects, and changes to ensure protection from start to finish of a service. To do this, we will need to improve workflow processes around assessments and authorization to support project requests and not delay

activities. Projects need to incorporate cybersecurity checks into project plans like they do for other activities, such as unit testing and Q&A testing.

In order to accomplish improved IT risk management, we need to:

- Enhance the IT Risk management program university wide.
- Define the scope and objectives of the policy, taking into account the unique characteristics of the higher education environment.
- Enhance the guidelines and procedures for the management of digital assets, including data classification, access controls, and retention policies.
- Identify and assess the risks associated with digital assets and develop strategies to mitigate those risks.

This will also need to include growing a robust cybersecurity infrastructure:

- Expand use of the security information and event management (SIEM) system across the university to monitor and respond to cybersecurity threats.
- Deploy advanced endpoint protection solutions to prevent and detect malware and other security threats.
- Conduct regular vulnerability assessments and penetration testing to identify and remediate weaknesses in the cybersecurity infrastructure.

- **Increase collaboration with other agencies, private sector industries and universities, especially UNC system schools**

Collaboration on IT tools, techniques, and warnings are critical to help keep attacks and breaches at bay. Other organizations face similar demands and threats, and collectively, we can approach solutions from a shared and more holistic approach. EDUCAUSE, Internet2, and other higher education-related groups offer platforms for sharing and learning about events, approaches, and actions that can help protect our data and resources while being efficient with our resources. Working with the UNC Information Security Council as well as other groups, can help reduce our risk by sharing ideas and solutions.

We need to enhance our partnerships with other higher education institutions, government agencies, and private sector organizations to share threat intelligence and best practices.

- **Improve the Cybersecurity funding model to account for growing IT risk management and compliance obligations**

  As the university and all businesses move more activities online and depend more completely on IT solutions, the risk to university functions and processes grows. Over the past 20 years, cybersecurity has become more complex with huge demands on resources to protect the university's data, intellectual property, and business activities.

  We can't just purchase tools and devices to buy our way to a safer environment. The needed resources (people, process, technology) include cyber tools, but also human effort, education, monitoring, and rapid support for issues.

  We must ensure we have the necessary dedicated, recurring funding to implement the most effective approaches to cyber protection.

- **Provide appropriate cybersecurity education and training for all members of the university community.**

  Currently, the number one cybersecurity risk is human. Phishing and behavioral approaches to hacking are dominating the successful attacks on IT systems. This means we need to be smart about our approach to protecting our assets. We need to ensure all employees and affiliates have proper cybersecurity training. Regular targeted training for all members of the community is needed to ensure everyone understands their roles and responsibilities on how to protect university IT resources.

  We need to foster a culture of cybersecurity awareness and education by:
  - Expand and implement a clear and comprehensive training program for students, staff, and faculty on cybersecurity and digital asset management.
  - Increase the cybersecurity awareness campaign to promote good security practices and raise awareness of emerging threats.
  - Provide more resources and tools to help individuals safeguard their digital assets.

GOAL: Leverage data across the university

The use of data to understand business processes, student success, research effectiveness, space use, and more has helped the university become more effective and efficient. Recognition

of the value of data as a business asset is emphasized in goal five of the university's strategic plan - Wolfpack 2030: Powering the Extraordinary with the statement "NC State commits to utilizing actionable intelligence to engage in more strategically focused planning and decision-making activities that benefit our students, staff, faculty, partners and the broader community." OIT plays a critical role in supporting this commitment.

It is imperative that the university formalize and make integral to our institutional culture the practice of data governance, which is the process of managing the availability, usability, integrity, and security of the data in enterprise systems. Further, there is a need for university-level facilitation around the access and use of university data as a business asset. OIT will partner with other central offices and campus stakeholders in both of these critical needs.

Strategies:

- **Leverage and enhance the university data governance structure to address data access, quality, security, and usage.**

  Data governance recognizes institutional data as a business asset and seeks to manage, protect, and leverage it as such. Data governance provides a coordinated approach to ensuring that data resources are accurate, consistent, understandable, accessible, and used appropriately. It enables the exercise of control and defines decision rights and authority with respect to institutional data.

  Work began in the fall of 2022 in partnership with leadership in Institutional Strategy and Analysis (ISA) to review issues related to data and data access and the functionality of our current university-wide data governance structure. Enhancements will reconsider the structure, membership, and roles of responsibility of our current structure and make recommendations as required. The review may also recommend the establishment of additional working groups and initiative teams intended to support the implementation of university-wide data governance.

- **Facilitate the access and use of university data as a business asset through coordinated implementations across the university.**

  The university implementation plan articulates four initiatives that are relevant to facilitating access and use of university data as a business asset. They are:

  - Identify and address gaps in our data analytics structures, platforms, and technologies.
  - Develop and maintain an accessible university data catalog to promote access to and shared understanding of data resources and consistent documentation, usage, and methodologies.

- Expand the number and scope of dashboards, reports, and other central data resources through coordinated efforts across the university that provide actionable information to decision-makers at all levels and the campus community.
- Provide training and outreach to the university community to promote access, usage, and data literacy with respect to institutional data and reports for decision-making.

OIT will support these initiatives as appropriate in partnership with other central offices and campus stakeholders to ensure coordinated implementation at the university level. These initiatives should greatly improve the utility and use of institutional data as a business asset.

GOAL: Grow IT resources appropriately to support Digital Transformation

It is important to fund universitywide IT to match its growing role in supporting the core university's mission and enabling the university to achieve its technology-infused strategic plan. Concurrent with recognizing the need to fund the technology and IT services that drive the university, IT groups need to be good stewards of the funds they have and manage. We must work across the university to find ways to be efficient with resources (people, software, and hardware) through reducing duplication, sharing positions, and using governance to collaborate for success.

Strategies:

- ### Execute an external review of IT positions, funding, and salaries across the university

  The university is a large and distributed environment. We have grown organically and have not implemented an organizational review across IT to understand support and funding levels as well as opportunities to meet the growing demand for services. While we have governance that works to balance the services between at-scale needs (generally at the enterprise level) versus local needs that are specialized and bespoke, an external review would provide a balanced look at our progress.

  The university also needs to understand and plan better to support IT career paths to attract and retain the quality talent we are accustomed to and will be in higher demand in the future. This includes reviewing IT salaries and market competitiveness in collaboration with our HR partners.

- **Look for economies of scale for commonly used software and services**

  Software license costs are going up while IT budgets are generally remaining flat. At the same time, the demand for more automated and efficient solutions is growing. Budgets, support, and tool access differ greatly across the university and can be even more problematic at remote locations. Frequently, software and service decisions are made in different time periods and result in a number of different tools and implementations.

  In order to be fiscally efficient, our distributed IT groups need to work to standardize software solutions for common categories. This might be accomplished by creating categories for software solutions and agreeing on a limited set of supported solutions. We must prioritize spending on each category based on the value to the university mission, the strategic plan, and risk reduction.

  We also need to improve training on financial tools to help IT groups verify and compare the total cost of ownership and the benefits of shared opportunities. Funding a universitywide review of IT support, tools, and common needs to identify possible savings might benefit developing shared opportunities.

- **Institute review processes and checkpoints to ensure the uniqueness and value of adding new tools or services**

  With the growth of Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS), Infrastructure-as-a-Service (IaaS), it has become easy to launch new solutions that are perceived as easy, low cost and efficient. However, often these solutions are duplicates of existing solutions, cost more than advertised to integrate into existing university tools, and put a support demand on units across the university. It is critical that we work together to develop review, approval, and funding processes that ensure value and proper understanding of the resources needed.

  One step towards this type of review is the IT Purchase Compliance (ITPC) review. This process ensures that any new SaaS, PaaS, IaaS, or IT-related purchase meets cybersecurity and accessibility policy. However, this does not review the uniqueness and sufficient differentiation from existing tools nor does it work towards finding common solutions across the university to reach scale and effectiveness.

  The IT Governance committees also provide a review process with different levels of effectiveness and compliance. The new Data Governance processes show promise in the use of data across the university.