

## IT Projects/Issues/Concerns to Address

1. Align business practices and then align technology with those business practices by developing and applying appropriate technology strategies.
2. Establish annual and midterm priorities/budgets to drive work and ensure accountability.
3. Immediately address the disconnects between Statewide OIT, campus IT, and campus end users.
4. Immediately address Banner operation dysfunctions including: governance, work backlog, access, cost.

Banner Upgrade: Ellucian has announced the deprecation of Banner 8 and advised all customers to make the transition to Banner 9 by December 2018. There are many modules and business processes that need to be reviewed and migrated.

Page Up: completing Banner/HR integration

CRM: Enrollment Rx-fully integrate CRM with banner.

Videoconference Service: Review of Videoconference service and plan for next generation of Videoconferencing to meet a variety of needs.

Neverending requests for Banner modifications.

TOP 1 - Blackboard sucks as it fails numerous times.

---

TOP 1 – Gmail is ridiculously bad for enterprise-level organizations.

---

1. Classrooms are not equipped for the 21st century in almost too many ways to mention. All but the smartest (latest) smart classrooms are outdated (but at least I know where to play my VHS tapes). Classes are not generally equipped for 2-way or even 1-way audio/video. Wireless networks sometimes work, sometimes not. **Projector bulbs are not generally stocked and can take a week or more to replace.... never had this problem with overhead transparency machines!**

2. University-licensed software (e.g. matlab) on university-provided machines (especially laptops) need network license check-outs or VPN. License nags to reduce check-outs, such as Acrobat preventing opening a few pdfs and reading them throughout the day.

3. Cannot assume some base level technology that students will have in the classroom

4. Yes, Blackboard sucks .... but alternative LMSs are not necessarily less expensive (e.g. Canvas) or better overall.

---

1. Frequent Blackboard outages

2. Wi-Fi signal too weak to stream online resources in classrooms
  3. Unreliability of A/V equipment in classrooms (not sure if this is an IT issue)
  4. Cannot access voicemail messages from email anymore
  5. Likely reduction of availability of people to fix IT problems (I have not been personally affected, but we no longer have an on-call IT guy at our college and we have to get these resources from IT. Are there enough of these resources to go around?)
- 

- 1) Functionality lost by switching to Gmail
  - 2) Blackboard outages
  - 3) Not enough bandwidth
  - 4) Lack of support/data/communication from Statewide IT Services
  - 5) Banner inflexibility
- 

1) Service response time/reliability, 2) micromanagement and limitations of program (e.g. EndNote, SigmaPlot, etc) availability, 3) BB outages, 4) voicemail notifications via email, 5) clarity regarding PC refresh process

### **1. Read access to institutional data**

This “pain point” is so extreme that I think it borders on an example of “waste, fraud and abuse.” Effectively, we have a cottage industry at UA dedicated to locking down access to non-confidential data. This includes the absurd examples I cited last week such access to the table which contains the names of campus buildings. Requests to gain access to non-confidential data are often denied. When they are accepted, often it requires intervention at the highest levels of the organization, routing through multiple committees, then implementation by highly-paid professionals.

I would argue that this is pure waste which borders on misuse of public funds. This is not something to be tweaked. The current security model needs to be thrown out.

The current model is based on the premise that all data must be locked down and access is granted on a very granular level and only after exhaustive review. I propose the following revolutionary approach: All data is accessible to UA staff unless it has been categorized as protected. Reversing the current paradigm: Data can be restricted, but only at a very granular level and only after careful review.

Protected categories should be based on explicit legal requirements. Example would include:

- Health records protected under HIPPA data
- Educational records protected under FERPA
- Personally identifiable information protected under (numerous statutes)
- Financial data protected under (numerous statutes)
- There are more, but I doubt there are many more.

Access to protected data should be granted at the category level. In other words, once you have been trained and approved to have access to a category (say, FERPA), the professional expectation is that you will comply with FERPA. Further **\*technological\*** constraints are not to be required. If employees do not comply, then this can be addressed as an HR issue.

This change would reduce the number of security classes from thousands down to under a dozen. Maybe under a half-dozen. It would save tens of thousands of staff hours, and encourage more strategic use of the ERP.

## **2. Write access to institutional data**

This is very different than #1. It is recognized that UA needs to have many controls to ensure the integrity of institutional data. Having said that, the current model prevents trained staff from being able to set up automation/data bridges. My favorite example was UAS' four year quest to be able to update employee telephone numbers. The current approach results in data not being updated and automation initiatives failing.

The solution is to have UA focus on having and enforcing clear data standards, but empowering our trained IT staff to support these standards through automation, etc.

## **3. Merged roles (mainly, employee-student)**

In days gone by, UA recognized that an individual may have distinct, non-overlapping roles with UA. The prime example being, I can be both an employee and also a degree-seeking student. These roles were compartmentalized in our information system.

In the early 2000s, this distinction was tossed out. This was a mistake which has caused many challenges. On an individual level, it creates challenges as institutional records (owned by the employer) are intermixed with academic records (protected by FERPA) and even personal records. This mixing makes it all but impossible to secure institutional data as employees change roles and come and go from the institution. It also creates challenges in ensuring student rights are appropriately protected.

Finally, this "merging" has resulted in a one-size-fits-all approach to our IT systems where we either seek to implement business-based best practices which are not appropriate for students, or we implement systems around the needs of our students which is inappropriate for employees in a business.

The solution is to work towards a disentanglement of roles.

## **4. Lack of a basic policy/guidance framework**

This relates to most of the items above, but especially the last point on merged roles. Due, in part, to the confusion of merged roles, UA has failed to develop clear guidance and policies about many or most basic services. A simple example would be e-mail. Nearly every modern business has well-established policies concerning how e-mail is to be used, what expectations of employees are, etc. This is nearly non-existent at UA.

1) limitations on quality of service for campuses and regional communities. Broadband is getting closer, but not for all rural communities. 2) Onsite IT support is limited. This is a UA community campus-wide concern. Some universities allocate funding for IT based on enrollment, which is insufficient, but others campuses don't have funding available for even a portion of staff/faculty for IT support.

**Response to: What are the top 5 IT "pain points", roadblocks or opportunities for improvement, from the perspective of your area?**

**1) Meet the first charge of the Information Technology Council: "Establish IT policy and administrative and operational standards"**

- In alignment with the adopted objectives of the ITC's charter, e.g. articulating priorities in support of mission, and decision authority cut points relative to cost, scope, stakeholder and/or customer impact, etc.
- Adopt a process and timeline to reach completion

**2) UA/UAA/UAF/UAS Executive level commitment (genuine, broad and sustained over multiple years) to utilize and support the Project Management function and its operations in accordance with standard best practices:**

- Transparent, inclusive, complete project vetting, prioritization and planning functions, used for all projects of a minimum scope and magnitude, as defined in IT policy and administrative and operational standards (item 1).
- Transparent project portfolio management, connecting resource planning with project execution

**3) Include IR as a primary stakeholder and/or customer in potential modifications to data and applications environment, to prevent data discontinuity and allow UA's data architecture development, maintenance and BI needs to be met** (in accordance with cut point criteria defined in IT policy and administrative and operational standards (item 1)). IR function is responsible to set data and data architecture standards to meet trend reporting, operational analysis, and compliance needs. Items to address in this area include, for example:

- Communicate when applications are being adopted and how data will articulate with Banner – whether data source is SaaS or locally hosted, transparency on data structure and how it will articulate; include addition of RPTP snapshots of databases/applications not intended or possible to articulate to Banner, i.e. Adirondack, Lumens, Raiser's Edge, defined to meet IR's and their customer's needs as part of application implementation plan.
- Maintain easily accessible living technical documentation for core data services/products such as RPTP data refresh schedules, reports schema, data structures for RPTP snapshots of Banner, Lumens, Adirondack data, etc.
- When programmers are requested to modify Banner, ensure IR and other stakeholders are consulted and informed, i.e. web time entry solution changed how data flows through Banner, causing surprise issues and rework for IR.
- Expanded management/archiving of RPTP tables and other data services through automated ETL of daily snapshots, allowing for year-over-year operational analysis, i.e. cubes or snapshots with value added fields.
- Support IR in attaching visual analytic software (e.g., dashboards, business intelligence tools) directly to RPTP.

**4) Communication & Setting Realistic Expectations.** Providing information that is understandable and accurate will prevent any perception of a lack of responsiveness.

- Identify key points of contact for each IT function, at UA, UAF, UAA and UAS. This allows for development of relationships and understanding between IT personnel and IR (or any other function's) personnel.

- Set and clearly communicate realistic service level and timing expectations, updating customers as needed
- Translate the IT organizational structure, functions and responsibilities to layperson speak and communicate to the UA community - explain what IT leaders and staff across the whole system actually do, and indicate who is responsible for what. Right now, organizational structure is stated in undefined IT terms that laypeople (and many others) do not understand or relate to.