A Case Study:

Implementing an Automated System for Processing Contracts in a Higher Education Institution

by:
Allie O'Connor and Catherine Susman

MIM 515
Spring 2015
Dr. Katie Pittman

School of Business
Southern Oregon University

June 9, 2015

Table of Contents

Introduction

Higher Education is big business. World-wide, governments spend more than $3.5 trillion annually on education (Chui, et al., 2013). In the United States alone, the government spends $800 billion per year to support 80 million full-time students (Regalado, 2013). According to Cota, Jayaram, and Laboissiere (2011), the United States "will need an additional one million [college graduates] per year by 2020 to sustain its economic health." Cota, et al. estimate the cost for the additional graduates to be at least $52 billion annually. This estimate is based on 2008 tuition costs. In an era marked by decreased government funding, now more than ever for higher education to remain big business, higher education must remain operationally and strategically positioned to remain competitive. To do that, higher education must look to technology to assist in gaining a sustainable competitive advantage.[1]

As Gallaugher (2014) notes, "technology has permeated every management discipline" (p.11). Similarly, technology, in all aspects of higher education, is the key to relevance. Winners and losers in the competition for students, grant and tuition dollars, and donations will be defined by an institution's ability to leverage technology in key areas of higher education's value chain. Key areas of the higher education value chain include delivery of academic content as well as the operations supporting the delivery of academic content.

Purchasing and contracting services is one of the many operational areas that support the delivery of academic content and the fulfillment of a university's mission. At the University of Oregon (UO), the Purchasing and Contracting Services (PCS) department's mission reflects this purpose. PCS' mission is "[s]upport [UO] and its mission by providing efficient and effective business services through securing assets and services for the University with best business practices" (University of Oregon Purchasing and Contracting Services, 2015). Just as universities must look to technology so to must the individual operational areas such as PCS.

This paper will provide a case study on the selection and implementation of technology by PCS in order to automate intake and reporting functions related to contracting at UO. As part of this case study, we will examine the following: (i) the regulatory environment and the related security issues and requirements; (ii) harnessing data through the use of analytics; (iii) two prior technology implementations at UO to provide a guide as effective implementation; and (iv) effective technology implementation strategies.

Background

UO is a public research institution with a Fiscal Year (FY) 2013[2] expenditure exceeding $773 million. (University of Oregon Office of Institutional Research, 2014). Of that $773 million, expenditures with third-party vendors for goods and services exceeded $129 million (University of Oregon, 2014). One department, PCS, managed those third-party

[1] Gallaugher (2013) defines sustainable competitive advantage as "financial performance that consistently outperforms . . . industry peers" (p. 22).
[2] FY2013 began July 1, 2012 and ended June 30, 2013.

vendor business transactions.[3] That processing function resulted in negotiating, drafting, and approving more than 4000 contracts and 2000 purchase orders, and reviewing tens of thousands of credit card transactions. UO like many higher education institutions still heavily relies on manual, human capital intensive procedures to process these business transactions.

UO currently utilizes manual data entry into shared Microsoft® Excel spreadsheets to track work flow and other dashboard data. This is a time and labor-intensive process, prone to data entry errors and platform instability. PCS has encountered repeated Microsoft® Excel spreadsheet failures resulting in a loss of data and increased demand on staff time. According to Olshan (2013) "[E]rrors in spreadsheets are pandemic" (para 3). Olshan notes that [c]lose to 90% of spreadsheet documents contain errors" (para 2). Furthermore, "the large spreadsheets with thousands of formulas [contain] dozens of undetected errors" (para.2).

According to Cota, Jayaram, and Laboissiere (2011), costs may be lowered "by converting paper-based systems to electronic ones" (Improving efficiency in core support and services, para. 1). With this in mind, and recognizing the limitations of the current cumbersome system, in fiscal year (FY)[4] 2013, PCS requested and was secured a small, one-time budget allocation for acquisition, implementation, and maintenance of an alternative intake and reporting system.

Once the budget was secured and the funds were made available, PCS began the process of automating certain aspects of the contract workflow/dashboard reporting procedures. Recognizing implementing an information system includes more than just acquiring hardware and software, PCS planned this project to take up to two-years to allow for researching, acquiring and implementing the new automated system.

As part of the first step, during FY2014 PCS conducted research including a review of the various switching costs involved with implementing a new system. As Gallaugher notes switching costs include costs associated with staff learning a new system, ability to retain data from the current system, and costs associated with acquiring the new system (Gallaugher, 2014, p. 29).

PCS' research included examination of UO's campus culture with an understanding that there is a limited tolerance by staff and faculty for learning new administrative systems. The system, therefore, needed to be seamlessly integrated into current processes so that faculty and staff would accept and use the automated intake system.

In addition to parameters created by the need to keep learning costs to a minimum, the budget allocated for the project was minimal. The project was funded at $84,000. This $84,000 was required to cover acquisition and implementation costs as well as all system maintenance for up to three years.

[3] Based on information from internal dashboards maintained by UO Purchasing and Contracting Services department.

[4] UO's fiscal year begins on July 1st and continues through June 30th.

After careful research and conducting an open competitive process, UO chose an automated system that will build on existing technology systems while allowing future scalability of functions. This approach maximizes benefits by providing not only an automated system to replace manual processes, but also one that requires minimal learning on the part of users and minimal initial investment. By strategically implementing technology solutions to certain parts of the UO purchasing and contracting value chain, PCS will improve its operational effectiveness and will increase its sustainable competitive advantage.

Once chosen and during the development phase, PCS and the developers of the new automated system had to be cognizant of myriad laws, rules and regulations to which colleges and universities are subject. These regulatory schemes present challenges to fostering an open, collaborative learning environment that promotes student learning, peer production[5] and student engagement. The regulations also create challenges for business units seeking to support the academic areas.

With that in mind, all PCS staff coordinated closely with system developers to ensure the system was implemented in alignment with applicable rules and regulations. It was important that all staff, not just senior staff, coordinated with the system designers in order to ensure maximum functionality and usability.

Regulatory Requirements, Security and the Need for Collaboration

Those outside of higher education, including system developers, may incorrectly assume that higher education is protected from the stringent security requirements and regulations applied to such regulatory industries as banking, telecommunications, real estate development and leasing, and health care (Bates, 2011). The nature of services delivered as part of higher education mission includes banking, health care, and many other highly regulated industries. Most highly regulated industries have the freedom to limit access and use of the internet and social media and networking as a matter of course (Vaira, 2015). Higher education, however, does not have this freedom, even though it is highly regulated.

Common Regulations That Apply to Universities and Colleges

Any system development must be designed in a way to accommodate the fact that higher education institutions are awash in personally identifiable information. Such information includes health records, financial information, student records, and electronic communications to touch on but a few. Recognizing the potential consequences of inappropriate release of this personally identifiable information may pose, the US Congress has passed laws to protect information accumulated and maintained by colleges and universities. Common federal regulations applicable to higher education include the following:

[5] Gallaugher (2013) defines peer production as "users collaboratively work[ing] to create content, products, and services. [Peer production] includes social media sites, open source software, and peer-produced services, such as skype and BitTorrent, where the participation of users provide the infrastructure and computational resources that enable the service" (p. 139).

- ***Family Education Rights and Privacy Act*** (FERPA). FERPA "protects the privacy of student education records, to provide students with rights to inspect and contest their records, and to provide guidelines for dealing with inaccurate data by means of formal and informal hearings" (St. Petersburg College, 2015). Institutions of higher education adopt voluminous policies outlining, in exquisite detail, how to comply with the law.[6]

- ***Health Insurance Portability and Accountability Act of 1996*** (HIPAA) protects the privacy of "individuals health information participating in certain health coverage plans and governs the use and disclosure of certain [health care] records" (St. Petersburg College, 2015). Colleges and universities that have a health center, or are otherwise associated with a health care provider must comply with HIPAA. This requires highly developed policies, procedures, requirements and forms for communicating protected student health information.

- ***Communication Assistance for Law Enforcement Act*** (CALEA) is a 1994 federal act that "further defines the statutory obligations of telecommunication carriers to assist law enforcement in executing electronic surveillance pursuant to court order or other lawful authorization" (Federal Bureau of Investigation, 2011, para. 1). While this may not seem applicable to higher education, this law impacts any college or university that maintains its own telecommunications network. Specifically, the implications of who accesses and how they access the telecommunications network is governed by CALEA. Get it wrong and the institution may face a fine of up to $10,000 per day (Communications Assistance for Law Enforcement Act, 1994).

In addition to FERPA, HIPAA, and CALEA, colleges and universities are subject to myriad export control laws, the US Patriot Act; the Technology, Education and Copyright Harmonization Act (TEACH); the Electronic Communications and Privacy Act; Computer Fraud and Abuse Act; and the Graham-Leach-Bliley Act.

All of the above referenced regulations are included in the Code of Federal Regulations. Adding to the complex regulatory landscape for colleges and universities is the state and local regulatory construct that also regulates many of these same areas. All these regulations are complex and all carry significant fines and penalties for failure to comply.

Challenges to Operating in the Regulatory Environment in Higher Education

In light of the regulatory requirements, PCS needed to build a system that allows open, accessible environments to encourage academic exploration, student learning and engagement, and collaboration at all levels. Such collaboration and accessibility go to the core of any higher education institution's mission. Higher education has specifically designed its "information technology infrastructure in a way that embraces and supports

[6] The University of Oregon Office of the Registrar has adopted a 14-page policy in 12-point type to ensure FERPA compliance.

interconnectivity and digital communication" (St. Petersburg College, 2015). PCS' infrastructure must, likewise, support interconnectivity and digital communication. "Unlike private corporate networks, which, by their nature, are designed to be 'walled gardens'[7] of information, campus networks—due to the need to facilitate collaboration and provide access to information—generally are designed to be more open, and therefore more vulnerable to misuse" (Salomon, Cassat, & Thibeau, 2003, p. 3).

Exploitation of the Vulnerabilities

Such vulnerability to misuse is reflected in the increased incidences of cybercrimes and exposure to black hat hackers[8] targeting universities and colleges. A couple of examples from 2014 involve Indiana University and University of Maryland (Vaira, 2015). Indiana University's networks were hacked, resulting in security breach affecting more than 140,000 student records (para. 2). In that same year, the University of Maryland networks were hacked resulting in a security breach affecting at least 300,000 student records (para. 2). These security breaches are but the tip of the iceberg. According to the Privacy Rights Clearinghouse[9], higher education has historically endured higher incidents of security breach than other regulated industries. The following table[10] shows breaches by industrial sector and the number or records exposed from 2005 through 2014.

Industry Sector	Percentage of Reported Breaches with Known Records	Number of Reported Breaches	Average Number of Records Exposed per Breach
EDU	73%	727	27,509
GOV	63%	682	349,070
BSF	51%	560	1,420,533
NGO	45%	97	44,789
MED	43%	1,136	67,280
BSO	38%	551	1,041,668
BSR	38%	505	1,087,949

Such security breaches can result in significant economic loss and liability because of the myriad regulatory requirements under which universities and colleges operate.

Meeting the Challenge of Vulnerabilities

Recognizing these vulnerabilities, PCS needed to make sure the system was implemented in a way to protect against vulnerabilities. This is particularly important since the system will be a hosted system maintained on external servers. As Vaira (2015) notes colleges and universities may meet the challenges posed by the cyber

[7] Gallaugher (2013) defines a walled garden as "a closed network or single set of services controlled by one dominant firm" (p. 189).
[8] Gallaugher (2013) defines a black hat hacker as "a computer criminal" (p. 312). In other words, a black hat hacker breaks into computer systems with criminal intent (p. 312). According to Gallaugher the term "hack" may have positive or negative connotations depending on context.
[9] The Privacy Rights Clearinghouse (PRC) is a nonprofit 501(c)(3) corporation whose mission is to provide information and training to individuals and entities related to privacy protection.
[10] The PRC table found in Joanna Grama's article *Just in Time Research: Data Breaches in Higher Education* published by Educause Center for Analysis and Research.

vulnerabilities to misuse by implementing an overall cybersecurity strategy consisting of three prongs: “prevention, detection, and response” (para. 4).

1. **Prevention.** As noted above, colleges and universities, by their unique missions cannot operate as walled gardens. In order to meet their missions they must deliver services and operate in an open and collaborative environment. It is simply not feasible to expect faculty and students to refrain from open and collaborative cyber activities. As such colleges and universities must craft and implement security systems that prevent cyberattacks from taking place. Prevention measures include email filtering; installation and use of anti-virus software; deployment of firewalls; segregating highly confidential data, and ensuring that regular maintenance of all of the foregoing. These measures are a key to prevention of cyberattacks and security breaches (para. 5-7). Any prevention method adopted by colleges and universities cannot stymie the free-wheeling collaboration and sharing of information that defines university and college academic culture. If the prevention method fails to meet usability requirements, then faculty and students will avoid or bypass such prevention methods resulting greater risk of security breaches.

2. ***Detection.*** According to Vaira (2015) “[d]etection seeks to identify any threats that attempt to exploit cybersecurity weaknesses within the institution’s systems” (para. 8). The goal of detection is to catch cybersecurity threats as early as possible. Vaira notes that the earlier the detection the greater the likelihood of minimizing the damage and cost to the institution associated with information breach.

3. ***Response.*** By the nature of the open and collaborative culture promoted by the academic mission, colleges and universities can expect to be targeted for cyberattacks and to experience breaches in security. Institutions of higher education, therefore, must develop response plans that include (i) identification of the breach and prevention of its spread; and (ii) a construct within which to assess damages due to the breach; and (iii) identification of preventative measures and implementation of same to prevent similar breaches in the future (Vaira, 2015, para. 9). According to the PRC, of the educational institutions that reported security breaches, one-third of those institutions experienced repeat breaches (Grama, 2014).

With this three-prong approach to security in mind, PCS included the requirements listed in Appendix A as part of the contractual terms for building, hosting and maintaining the PCS automated system. Those requirements include prevention, detection, and response components. It is important to note, that as a public university responsibility for response compliance must be shared between the vendor and UO.

A Tale of Two Technology Implementations

PCS actions were informed by two prior UO technology implementations; one area provides an example of a successful analysis and implementation of technology; one area provides an example of a failure of implementation of technology.

The Successful Implementation

In 2012, UO recognized that its plethora of data was siloed. As a result, that data was not optimized to provide information to inform and support decisions of UO leadership. To remedy this issue, UO sought to acquire and implement a customer relationship management system (CRM)[11] that was scalable to allow phased implementation and promote a flatter hierarchy allowing greater direct access by staff to information and dashboard reporting. The CRM is allowing UO to better identify and target its recruitment activities resulting in greater enrollment of academically higher-caliber students. For example, in 2014 University's entering freshman class had a grade point average (GPA) of 3.58 while the 2010 GPA of the entering freshman class was 3.52 (University of Oregon Office of Enrollment Management, 2014). The CRM was implemented at the University in 2011- 2012.

The Unsuccessful Implementation

In contrast to the intentional process used to determine the best options for implementation of the CRM, the automation of payroll and timekeeping functions was undertaken by a department[12] that made the mistake of believing technology, by itself, was a panacea.

At the time of the ill-fated implementation, the UO department was using a timekeeping and payroll system that relied intensively on paper forms and manual data entry. Due to the current cumbersome process, the UO department undertook a project to automate these systems. The UO department identified a software system through a competitive process. The department was so enthusiastic about the potential of the new software, the department insisted on fast-tracking the purchase process. Similar to Gallaugher's example of Prada, the software system "sounded slick, but execution of the vision was disastrous." (Gallaugher, 2014, p. 47). The department identified hardware and software to automate its processes, but neglected to recognize that an information system also includes users of the system, data, and processes and procedures. The UO department also neglected to recognize there would be switching costs associated with the implementation of the new technology.

The result of this rush to embrace technology, without adequate analysis of the impact, resulted in a great software system. That great software system, however, did not integrate with existing processes or procedures, required too high of a learning cost for staff to use, and did not allow migration/conversion of essential data.

[11] According to Gallaugher (2014) a "CRM" systems used to support customer-related sales and marketing activities" (p. 219).

[12] The UO department and software vendor are intentionally not identified.

Effective Implementation of Technology in Higher Education

PCS wanted to avoid a technology project failure. Avoiding technology project failure is directly keyed to timing implementation at the appropriate process maturity level for the organization. There are many ways to calibrate an organization's process maturity level. One method of calibrating whether an organization is at the appropriate process maturity level for the chosen technology implementation is by application of a capability maturity model integration (CMMI). Gallaugher (2014) defines a CMMI as "[a] process improvement approach . . . that can assist in assessing the maturity, quality, and development of certain organizational business processes, and suggests steps for their improvement" (p. 229). Such maturity models often use human life cycle stages as a metaphor for organization development stages (e.g. infant, child, teenager, or adult) (Watson, 2013, p. 17).

Much like the success in implementation and use of analytics, there appears to be a direct correlation between success in implementation and the maturity level of the organization. With this in mind an organization contemplating technology implementation can look to Watson who provides a CMMI-type model specifically for gauging an organizations readiness and the level of technology appropriate to that maturity (Watson, 2013, p. 18).

Watson's (2013) prescription for implementation requires, as the first steps, consideration of each of the following factors:

(i) "A clear business need;
(ii) Strong, committed, sponsorship;
(iii) Alignment between the business and IT strategy;
(iv) A fact-based decision making culture;
(v) A strong data infrastructure;
(vi) The right analytical tools;
(vii) Strong analytical personnel in an appropriate organizational structure" (p.18).

Applying Watson's prescription for implementation facilitates an understanding of and defines a road map for determining whether an organization is sufficiently mature to successfully implement a technology project.

PCS did not have these seven considerations mapped at the commencement of the process. Examining the decision to move forward with a technology implementation process retrospectively, however, indicates each of these seven factors was considered and met. Specifically, PCS identified:

- The clear business need to acquire a less labor-intensive, more accurate intake and reporting process.
- This need was clearly articulated through a budget request process. Executive leadership approved the budget request articulating its commitment to PCS' acquisition of an appropriate technology system.
- PCS worked closely with executive leadership and internal information technology (IT) staff to ensure alignment between PCS' business needs and the existing IT infrastructure and IT staffing capabilities. This alignment analysis

revealed PCS, like many departments, had no internal IT staffing and was facing at least a two year wait for central IT support for the project. PCS, therefore, learned of the need to fully outsource this project.

- As part of the budget and approval process, PCS documented the need for a new more stable and accurate system. The competitive process then allowed for a transparent method of matching potential technology solutions to the exact issues PCS sought to resolve.
- While the PCS legacy system[13] was prone to instability, inaccuracies, and did not interface with any other existing UO IT infrastructure, it did maintain vast amounts of data related to purchasing and contracting at UO. That data allowed the creation of an array of descriptive analytics[14] for baseline benchmarking.
- In choosing a new technology system, PCS needed ensure the new system could maintain the current descriptive analytics as well as provide a platform upon which to develop predictive and prescriptive analytics.[15]
- While this project was a hosted, outsourced solution, PCS staffing decisions have still included a focus on analytical and technological ability.

Harnessing the Right Data using the Right Analytics for Higher Education

One of the main goals for PCS in undertaking the acquisition and implementation of the new technology system was to improve reporting accuracy and capabilities. As part of the process, therefore, existing data and additional information needs were extensively analyzed. Application of Gallaugher's (2014) six considerations for technology implementation focuses on data. The six considerations are as follows:

(i) Data relevance – what data should be harnessed;
(ii) Data sourcing – is the data obtainable? If so, how?
(iii) Data quantity;
(iv) Data quality – is the data accurate?;
(v) Data housing – where will the data be stored?; and
(vi) Data governance – what rules and procedures will apply to managing the data and the system (p.271).

Again, as with assessing PCS' maturity level, a retrospective review of the six considerations for the implementation process outlined by Gallaugher reveals that PCS' implementation included review and analysis of these above factors. For instance, one

[13] Gallaugher (2014) defines a legacy system as "[o]lder information systems that are often incompatible with other systems, technologies, and ways of conducting business. Incompatible legacy systems can be a major roadblock to turning data into information, and they can inhibit firm agility, holding back operational and strategic initiatives" (p. 268).

[14] Descriptive analytics seeks to define "what has occurred" (Watson , 2013, p. 13). Examples of descriptive analytics include "reporting, OLAP, dashboards/scorecards, and data visualization" (p.13). Descriptive analytics can be thought of as basic, run-of-the-mill data. This is commonly the first step in an organization's use of analytics.

[15] Predictive analytics provide a basis for "what will occur in the future" (Watson, 2013, p. 14). Examples of predictive analytics include regression analysis. Predictive analytics are the springboard for the third subset of analytics—prescriptive analytics. Prescriptive analytics reflect "what should occur" (p.14). Prescriptive analytics allow an organization to use information to optimize performance and services in order to achieve a sustainable competitive advantage.

of the first areas analyzed by PCS was data relevance. The question was whether migrating/converting existing data into the new automated system would result in a sufficient return on investment to support the expenditure. While the legacy system comprised of Microsoft® Excel spreadsheets was unstable for daily use, it would not be difficult to maintain for historical data purposes. Overall, the analysis revealed that migration/conversion of historical data would not be cost effective.

PCS recognized that successful use of analytics allows an organization to achieve a sustainable competitive advantage. As Watson (2013) notes "top performing companies use analytics five times more than low performing companies" (p.15).

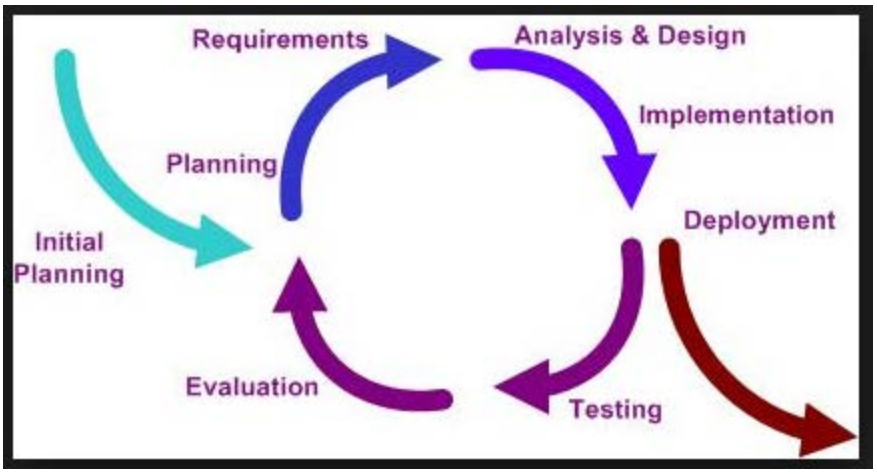
Higher education is modeling business practices from the corporate world. According to Guthrie (2013), smart higher education administrators recognize "that big data can be used in admissions, budgeting and student services to ensure transparency, better distribution of resources, and identification of at-risk students" (para. 7).

Testing Success

PCS is now entering the testing phase of the technology implementation project. During this phase, PCS and its system designer will undertake the testing phase simultaneously with the completion of the development phase. This simultaneous approach to testing, development and refinement is critical to success and ensuring usability[16] of the system. According to materials found on the usability.gov website, "[u]sabilty [e]valuation focuses on how well users can learn and use a product to achieve their goals. It also refers to how satisfied users are with that process" (Digital Communications Division (DCD), 2015).

Rather than a traditional stair-step or waterfall approach to design and deployment of a system, PCS is using an iterative and incremental development process that is a type of agile or rapid application development. The following image illustrates this approach.

[16] Materials contained on the website usability.gov define the term "usability" as "the quality of a user's experience when interacting with products or systems, including websites, software, devices, or applications. Usability is about effectiveness, efficiency and the overall satisfaction of the user" (Digital Communications Division (DCD), 2015).



(Anshu, 2011)

This iterative and incremental development approach will allow testing and evaluation to directly inform system design. The goal is to obtain a more functional and usable system in a shorter amount of time.

PCS will use the testing plan developed by usability.gov. A completed template for the testing of the new automated system is attached as Appendix B (Digital Communications Division (DCD), 2015).

The testing phase will be divided into two parts. Initially, PCS will conduct internal staff testing focused on website functional capabilities. Specifically, PCS staff will assess ease of use of the intake and reporting system. Once PCS staff have conducted the initial testing, not less than five and not more than ten campus users will be asked to use the website to submit documents to PCS for processing. The campus users' online experiences will be evaluated to determine usability of the website. As Nielsen notes, "the most important usability attributes are learnability and subjective satisfaction" (Nielsen, 2000, p. 270). Specifically, this evaluation will focus on three discrete areas identified by Bailey (2006) as critical for evaluation:

(i) Percent Correct (Effectiveness)
(ii) Time to Complete Each Scenario (Efficiency)
(iii) Satisfaction (Bailey, 2006, pp. 1-2)

As outlined in Appendix B, the effectiveness and efficiency of the new automated system will be automatically tracked and reported by the website. User satisfaction will be analyzed through a Qualtrics survey to be completed by each test participant at the end of the testing window. The Qualtrics survey will be developed using the questions contained in the attached Appendix C.

Conclusion

University of Oregon, like all institutions of higher education, can create a sustainable competitive advantage by integrating technology systems into its administrative and operational processes. All technology implementation must be done with mindful recognition of the risk of data breach and must take the initiative at leadership level to adopt, implement, and enforce data security protocols. The design and enforcement of

such protocols requires input from program elements, management elements and legal counsel, at a minimum.

In order to operate lawfully and with minimum risk of unintentional and unauthorized data disclosure and the mordant sanctions which may follow from such breaches, all institutions of higher education should insure broad institutional awareness of the applicable laws, risks of data breach, and community acceptance of the institutional safeguards and protocols designed and established.

Accomplishment of these objectives requires, at a minimum:

- Designing, adopting, and upgrading data safeguard programs and protocols which fit the specific systems of the institution;
- Educating and convincing the institutional community of the need for prevention of data breach, the potential consequences of data breach to the institution and the individual members of the community, and the requirement of following institutional data safeguard protocols;
- Committing appropriate and adequate resources to this educational project;
- Testing the safeguards on a random, cyclic basis to ascertain data security measures are operating and effective;
- Testing the level of attentiveness of the community to following the obligatory protocols; and
- Enforcing the protocols by appropriate action when/if there is a failure to follow the protocols.

While there is no system which cannot be hacked, design, adoption and credible enforcement of a program to protect the data which an institution must collect will mitigate data loss and attendant liability.

Adherence to recognized technology implementation constructs must be maintained in order to implement technology systems that allow and sustain a competitive advantage. Those constructs are briefly outlined in this paper and will guide UO PCS technology implementation activities.

References

Anshu. (2011, July 29). *System Development Life Cycle (SDLC)*. Retrieved May 30, 2015, from Java World: https://anshuchoudhury.wordpress.com/category/sdlc/

Bailey, B. (2006, March 1). *Getting the Complete Picture with Usability Testing*. Retrieved May 23, 2015, from usability.gov: http://www.usability.gov/get-involved/blog/2006/03/complete-picture-with-usability-testing.html

Bates, C. (2011, July 18). *Taking Your Information Security Program to the Next Level: A Higher Education Perspective.* Retrieved May 24, 2015, from Eller College of Management, The Univesity of Arizona: http://iasec.eller.arizona.edu/docs/whitepepers/take_info_security_to_next_level.pdf

Chui, M., Manyika, J., Bughin, J., Brown, B., Roberts, R., Danielson, J., & Gupta, S. (2013, May). *Insights & Publications.* Retrieved April 16, 2015, from McKinsey & Company: http://www.mckinsey.com/insights

Communications Assistance for Law Enforcement Act. (1994). *Pub. L. No. 103-414, 108 Stat. 4279*.

Cota, A., Jayaram, K., & Laboissiere, M. C. (2011, April). *Insights & Publications.* Retrieved April 18, 2015, from McKinsey & Company: http://www.mckinsey.com/insights/social_sector/boosting_productivity_in_us_higher_education

Digital Communications Division (DCD). (2015, March 27). *Online Surveys*. Retrieved May 23, 2015, from usability.gov: http://www.usability.gov/how-to-and-tools/methods/online-surveys.html

Digital Communications Division (DCD). (2015, March 27). *Usaability Test Plan Template*. Retrieved May 23, 2015, from usability.gov: http://www.usability.gov/how-to-and-tools/resources/templates/usability-test-plan-template.html

Digital Communications Division (DCD). (2015, March 27). *Usability Evaluation Basics*. Retrieved May 23, 2015, from usability.gov: http://www.usability.gov/what-and-why/usability-evaluation.html

Gallaugher, J. (2014). *Information Systems: A Manager's Guide To Harnessing Technology* (Version 2.0 ed.). Washington, DC, USA: Flat World Knowledge, Inc.

Grama, J. (2014). *Just in Time Research: Data Breaches in Higher Education.* Retrieved May 24, 2015, from Educause Center for Analysis and Research: https://net.educause.edu/ir/library/pdf/ECP1402.pdf

Nielsen, J. (2000). *Designing Web Usability: The Practice of Simplicity.* (S. Weiss, Ed.) USA: David Dwyer New Riders Publishing.

Olshan, J. (2013, April 20). *MarketWatch: 88% of spreadsheets have errors*. Retrieved May 30, 2015, from MarketWatch: http://www.marketwatch.com/story/88-of-spreadsheets-have-errors-2013-04-17

Regalado, A. (2013, January/February). Digital Education: The Most Important Education Technology in 200 Years. *MIT Technology Review, 116*(1), 61-62.

Salomon, K. D., Cassat, P. C., & Thibeau, B. E. (2003, March 20). *IT Security for Higher Education: A Legal Perspective.* Retrieved May 30, 2015, from Educause.edu: https://net.educause.edu/ir/library/pdf/CSD2746.pdf

St. Petersburg College. (2015, May 19). *Legalities Governing Information Security in Higher Education: HIPAA.* Retrieved May 24, 2015, from Legalities Governing Information Security in Higher Education: http://spcollege.libguides.com/c.php?g=254377&p=1695426

St. Petersburg College. (2015, May 19). *Legalities Governing Information Security in Higher Education: FERPA.* Retrieved May 24, 2015, from Legalities Governing Information Security in Higher Education: pcollege.libguides.com/c.php?g=254377&p=1695425

St. Petersburg College. (2015, May 19). *Legalities Governing Information Security in Higher Education: Home*. Retrieved May 24, 2015, from Legalities Governing Information Security in Higher Education: http://spcollege.libguides.com/infosechighered

University of Oregon. (2014). *Vendor Spending*. Retrieved April 2015, from University of Oregon Office of Institutional Research: http://ir.uoregon.edu/vendor

University of Oregon Office of Enrollment Management. (2014). *Annual Report*. Retrieved May 13, 2015, from University of Oregon Enrollment Management: http://oem.uoregon.edu/annual-report

University of Oregon Office of Institutional Research. (2014). *Office of Institutional Research: Expenditures*. Retrieved April 2015, from University of Oregon Office of Institutional Research: http://ir.uoregon.edu/expenditures

University of Oregon Purchasing and Contracting Services. (2015, May). *About Us: PCS Mission*. Retrieved May 30, 2015, from UO Purchasing and Contracting Services: https://pcs.uoregon.edu/content/about-uscontact

Vaira, P. F. (2015, May 19). *Protecting Against Cyperattacks on Colleges and Universities.* Retrieved May 23, 2015, from http://www.thelegalintelligencer.com/id=1202726786359/Protecting-Against-Cyberattacks-on-Colleges-and-Universities?slreturn=20150423180002

Watson , H. J. (2013, January-March). All About Analytics. *International Journal of Business Intelligence Research, 4*(1), pp. 13-28.

Appendix A

PCS Contractual Terms for Implementation, Hosting, and Maintenance of the PCS Automated Intake and Reporting System

Contractor will provide a Workflow Management System that includes the following:

1.1. Data Ownership and Security
  1.1.1. University is and will remain the owner of any and all data entered into the Workflow Management System
  1.1.2. University has the right to delete any data or request that it be deleted from the Workflow Management System at any time.
  1.1.3. University has the right to request an exported copy of any or all data from the Workflow Management System at any time.
  1.1.4. Contractor will make no use of data in any of the applications without express prior written consent from University.
  1.1.5. Contractor will provide a redundant cloud-hosted solution with all data stored within the United States.
  1.1.6. Security tools will include:
    1.1.6.1.1. 256-bit encryption any time data is being sent over a network or written to a disk
    1.1.6.1.2. Hardened Linux servers
    1.1.6.1.3. Multiple redundant cloud hosting providers
    1.1.6.1.4. Multiple redundant firewalls
    1.1.6.1.5. Intrusion detection systems (Tripwire)
    1.1.6.1.6. Security scanners (Nessus)
    1.1.6.1.7. Port scanners (nmap)
    1.1.6.1.8. Multiple security questions
    1.1.6.1.9. Customizable password policies upon request by University
    1.1.6.1.10. Multiple-factor authentication upon request by University
1.2. Maintenance and Support will include error fixes, maintenance, upgrades and enhancements during the term of this Contract
1.3. Backup and Recovery
  1.3.1. Daily incremental and monthly full backups which are fully encrypted before data is archived.

Appendix B

UNIVERSITY OF OREGON
PURCHASING AND CONTRACTING SERVICES
AUTOMATED INTAKE AND REPORTING PROJECT

Usability Test Plan
(Using template Usability Test Plan from www.usability.gov)

Version 1.0

Catherine Susman, Director
Allie O'Connor, Associate Director
June 9, 2015

Table of Contents

Document Overview

This document describes a test plan for conducting a usability test during the development of the University of Oregon (UO) Purchasing and Contracting Services (PCS) automated intake and reporting system (the Intake System). The goals of usability testing include establishing a baseline of user performance, establishing and validating user performance measures, and identifying potential design concerns to be addressed in order to improve the efficiency, productivity, and end-user satisfaction.

The usability test objectives are:

- To determine design inconsistencies and usability problem areas within the user interface and content areas. Potential sources of error may include:
  - Navigation errors – failure to locate functions, excessive keystrokes to complete a function, failure to follow recommended screen flow.
  - Presentation errors – failure to locate and properly act upon desired information in screens, selection errors due to labeling ambiguities.
  - Control usage problems – improper toolbar or entry field usage.
- Exercise the web site under controlled test conditions with representative users. Data will be used to access whether usability goals regarding an effective, efficient, and well-received user interface have been achieved.
- Establish baseline user performance and user-satisfaction levels of the user interface for future usability evaluations.
- Establish system ability to provide analytics and dashboard reporting

The user group engaged for this usability study will consist of two cohorts. The first cohort will consist of all internal PCS staff. The second cohort will consist of not less than five and not more than ten campus users.

Testing will take place internally at PCS and externally in users' departments across campus.

Testing of both cohorts is anticipated to take place over summer 2015.

Executive Summary

The PCS Intake System will provide a streamlining of the process for intake of contracts and other matters to PCS. Additionally, the PCS Intake System will provide dashboard reporting and analytics to facilitate process management. Critical to the success of this technology implementation is user acceptance of the PCS Intake System.

This usability study will examine the effectiveness, efficiency and user satisfaction with the new PCS Intake System.

Upon review of this usability test plan, including the draft task scenarios and usability goals for the PCS Intake System, documented acceptance of the plan is expected.

Methodology

As noted above, the user group engaged for this usability study will consist of two cohorts. The first cohort will consist of all internal PCS staff. The second cohort will consist of not less than five and not more than ten campus users.

Testing will take place internally at PCS and externally in users' departments across campus.

Testing of both cohorts is anticipated to take place over summer 2015.Not less than five and not more than ten campus users will be recruited to test the new PCS Intake System.

Through the PCS Intake System the timing and accuracy of user responses will be tracked and reported. Additionally, users will be asked to complete a satisfaction survey using Qualtrics to record their overall experience with the PCS Intake System.

Participants

All internal PCS staff members will test those parts of the PCS Intake System that relate to their specific job duties. In other words, PCS staff members will test those parts of the system that they are required to use daily in order to execute their job duties.

External testing will be undertaken by a variety of campus users. A particular focus will be on recruiting two cohorts of external users. The first cohort will consist of those who routinely submit more than 50 contracts per year to PCS. The second cohort will consist of those who submit fewer than 10 contracts per year to PCS.

The participants' responsibilities will be to attempt to complete a set of representative task scenarios presented to them in as efficient and timely a manner as possible, and to provide feedback regarding the usability and acceptability of the user interface. The participants will be directed to provide honest opinions regarding the usability of the application, and to participate in post-session subjective questionnaires and debriefing.

Training

PCS expects the new PCS Intake System to be intuitive. External users will attend a 30-minute orientation in the PCS conference room (by Skype or in person). The orientation will include system user instructions and an outline of testing procedures and objectives.

Procedure

Participants will take part in the usability test via logging into the PCS Intake System test environment. The participant will be seated at their workstation in their work environment. Verbal communication will be supported via telephone.
All participants will be advised of a testing window during which they can log onto the test system to complete a predesigned set of tasks.

After each task, the participant will complete the post-task Qualtrics survey and elaborate on the task session. After all tasks have been attempted, the participant will complete a post-test satisfaction Qualtrics survey.

Roles

The roles involved in a usability test are as follows. An individual may play multiple roles and tests may not require all roles.

Trainer

- Provide training overview prior to usability testing
- Defines usability and purpose of usability testing to participants
- Assists in conduct of participant and observer debriefing sessions
- Responds to participant's requests for assistance

Data Logger

- The test system will automatically record participant’s actions.

Test Participants

- Complete the predesigned set of tasks and Qualtrics surveys.

Ethics

All persons involved with the usability test are required to adhere to the following ethical guidelines:

- The performance of any test participant must not be individually attributable. Individual participant's name should not be used in reference outside the testing session.
- A description of the participant's performance should not be reported to his or her manager.

Usability Tasks

Each participant will be asked to complete the following tasks:

- A submittal request for a purchase order.
- A submittal request for a personal services contract.
- A submittal request for a facilities use agreement.
- A submittal request for a custom contract
- A submittal request for a request for quotes.
- A submittal request for an alternative procurement.

Three PCS staff members will be asked to perform the following additional tasks:

- Prepare a dashboard report of all monthly submittals by type of matter.
- Prepare a dashboard report of processing time for all matters by type of matter.

- Prepare a report of all matters by status of such matter.
- Prepare a dashboard report of all matters by staff member assignments.

Usability Metrics

Usability metrics refers to user performance measured against specific performance goals necessary to satisfy usability requirements. Scenario completion success rates, adherence to dialog scripts, error rates, and subjective evaluations will be used. Time-to-completion of scenarios will also be collected.

Scenario Completion

Each scenario will require, or request, that the participant obtains or inputs specific data that would be used in course of a typical task. The scenario is completed when the participant indicates the scenario's goal has been obtained (whether successfully or unsuccessfully) or the participant requests and receives sufficient guidance as to warrant scoring the scenario as a critical error.

Critical Errors

Critical errors are deviations at completion from the targets of the scenario. Obtaining or otherwise reporting of the wrong data value due to participant workflow is a critical error. Participants may or may not be aware that the task goal is incorrect or incomplete.

Independent completion of the scenario is a universal goal; help obtained from the other usability test roles is cause to score the scenario a critical error. Critical errors can also be assigned when the participant initiates (or attempts to initiate) and action that will result in the goal state becoming unobtainable. In general, critical errors are unresolved errors during the process of completing the task or errors that produce an incorrect outcome.

Non-critical Errors

Non-critical errors are errors that are recovered from by the participant or, if not detected, do not result in processing problems or unexpected results. Although non-critical errors can be undetected by the participant, when they are detected they are generally frustrating to the participant.

These errors may be procedural, in which the participant does not complete a scenario in the most optimal means (e.g., excessive steps and keystrokes). These errors may also be errors of confusion (ex., initially selecting the wrong function, using a user-interface control incorrectly such as attempting to edit an un-editable field).

Noncritical errors may be recovered from during the process of completing the scenario. Exploratory behavior, such as opening the wrong menu while searching for a function, will be coded as a non-critical error.

Subjective Evaluations

Subjective evaluations regarding ease of use and satisfaction will be collected via Qualtrics surveys, and during debriefing at the conclusion of the session. The Qualtrics surveys will utilize free-form responses and rating scales.

Scenario Completion Time (time on task)

The time to complete each scenario, not including subjective evaluation durations, will be recorded.

Usability Goals

The next section describes the usability goals for PCS Intake System.

Completion Rate

Completion rate is the percentage of test participants who successfully complete the task without critical errors. A critical error is defined as an error that results in an incorrect or incomplete outcome. In other words, the completion rate represents the percentage of participants who, when they are finished with the specified task, have an "output" that is correct. Note: If a participant requires assistance in order to achieve a correct output then the task will be scored as a critical error and the overall completion rate for the task will be affected.

A completion rate of 100% is the goal for each task in this usability test.

Error-free rate

Error-free rate is the percentage of test participants who complete the task without any errors (critical **or** non-critical errors). A non-critical error is an error that would not have an impact on the final output of the task but would result in the task being completed less efficiently.

An error-free rate of 80% is the goal for each task in this usability test.

Time on Task (TOT)

The time to complete a scenario is referred to as "time on task". It is measured from the time the person begins the scenario to the time he/she signals completion.

Subjective Measures

Subjective opinions about specific tasks, time to perform each task, features, and functionality will be surveyed. At the end of the test, participants will rate their satisfaction with the overall system. Combined with the interview/debriefing session, these data are used to assess attitudes of the participants.

Problem Severity

To prioritize recommendations, a method of problem severity classification will be used in the analysis of the data collected during evaluation activities. The approach treats problem severity as a combination of two factors - the impact of

the problem and the frequency of users experiencing the problem during the evaluation.

Impact

Impact is the ranking of the consequences of the problem by defining the level of impact that the problem has on successful task completion. There are three levels of impact:

- High - prevents the user from completing the task (critical error)
- Moderate - causes user difficulty but the task can be completed (non-critical error)
- Low - minor problems that do not significantly affect the task completion (non-critical error)

Frequency

Frequency is the percentage of participants who experience the problem when working on a task.

- High: 30% or more of the participants experience the problem
- Moderate: 11% - 29% of participants experience the problem
- Low: 10% or fewer of the participants experience the problem

Problem Severity Classification

The identified severity for each problem implies a general reward for resolving it, and a general risk for not addressing it, in the current release.

Severity 1 - High impact problems that often prevent a user from correctly completing a task. They occur in varying frequency and are characteristic of calls to the Help Desk. Reward for resolution is typically exhibited in fewer Help Desk calls and reduced redevelopment costs.

Severity 2 - Moderate to high frequency problems with moderate to low impact are typical of erroneous actions that the participant recognizes needs to be undone. Reward for resolution is typically exhibited in reduced time on task and decreased training costs.

Severity 3 - Either moderate problems with low frequency or low problems with moderate frequency; these are minor annoyance problems faced by a number of participants. Reward for resolution is typically exhibited in reduced time on task and increased data integrity.

Severity 4 - Low impact problems faced by few participants; there is low risk to not resolving these problems. Reward for resolution is typically exhibited in increased user satisfaction.

Reporting Results

The Usability Test Report will be provided at the conclusion of the usability test. It will consist of a report and/or a presentation of the results; evaluate the usability metrics against the pre-approved goals, subjective evaluations, and specific usability problems and recommendations for resolution. The recommendations will be categorically sized by development to aid in implementation strategy.

Appendix C
Qualtrics Survey Questions

Using the following questions suggested on the website usability.gov, PCS will create a Qualtrics survey for all test participants:

- Were you able to find the information you seek in the new Intake System?
- How satisfied are you with the new Intake System?
- What did you like about the new Intake System?
- What did you dislike about the new Intake System?
- What frustrations or issues did you have with the new Intake System?
- Do you have ideas or suggestions for improvements to the new Intake System?