Youngstown
STATE UNIVERSITY

BOARD OF TRUSTEES
AUDIT SUBCOMMITTEE
Leonard D. Schiavone, Chair
James E. "Ted" Roberts, Vice Chair
Carole S. Weimer
David C. Deibel
Samantha P. Anderson

Wednesday, March 15, 2017
1:30 p.m. or immediately following previous meeting

Tod Hall
Board Meeting Room

AGENDA

A. Disposition of Minutes for Meeting Held November 30, 2016

B. Old Business

C. Committee Items

1. Discussion Items

a. YSU Anonymous Reporting Line
Sarah Gampo, Director of Internal Audit and Risk Management, will report.

Tab C.1.b. **b. Audit Timeline Matrix**
This matrix tracks the progress of the implementation of recommendations for improvement or correction made by internal and external auditors.
Sarah Gampo, Director of Internal Audit and Risk Management, will report.

Tab C.1.c. **c. Updated on FY17 Internal Audit Plan**
Sarah Gampo, Director of Internal Audit and Risk Management, will report.

Tab C.1.d. **d. Annual Cyber Security Update**
Chris Wentz, Associate Director and Information Security Officer, will report.

2. Action Item

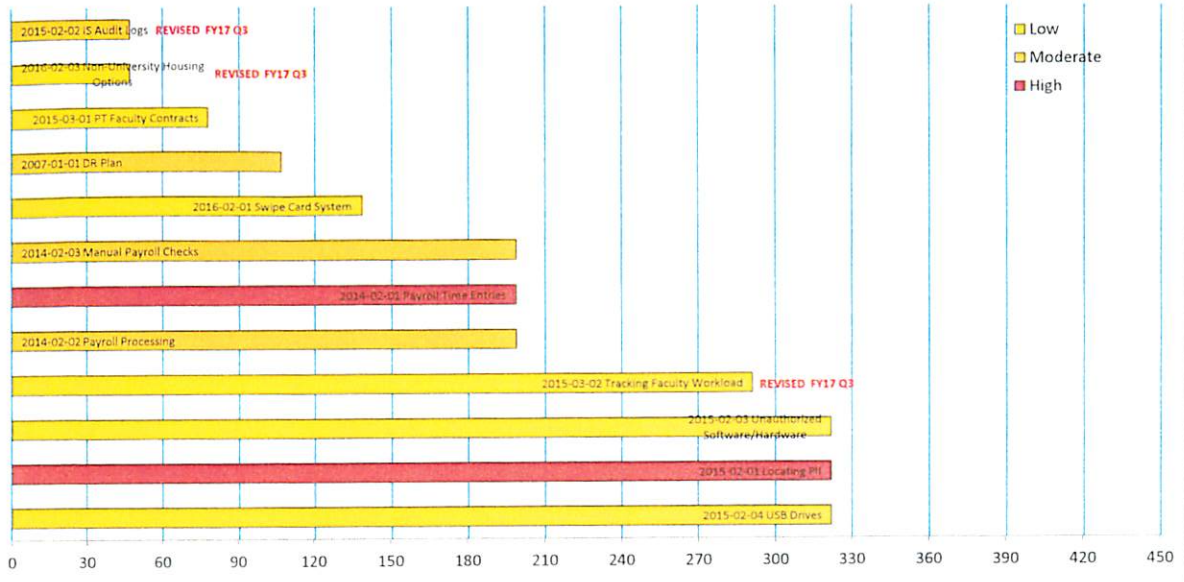
Tab C.2.a. **a. Resolution to Modify the Name of the Office of Internal Audit and Risk Management**
Sarah Gampo, Director of Internal Audit and Risk Management, will report.

D. New Business

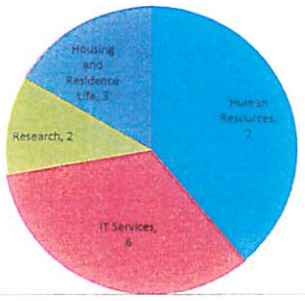
E. Adjournment

AUDIT RECOMMENDATIONS DASHBOARD
3rd QUARTER FISCAL YEAR 2017

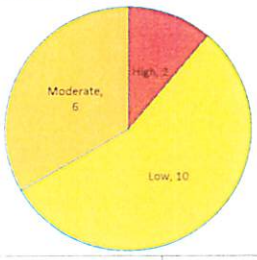
Audit Recommendations - Days to Current Deadline from 3/15/17



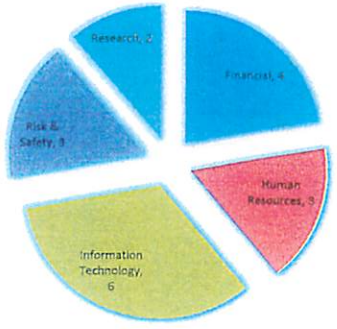
Department



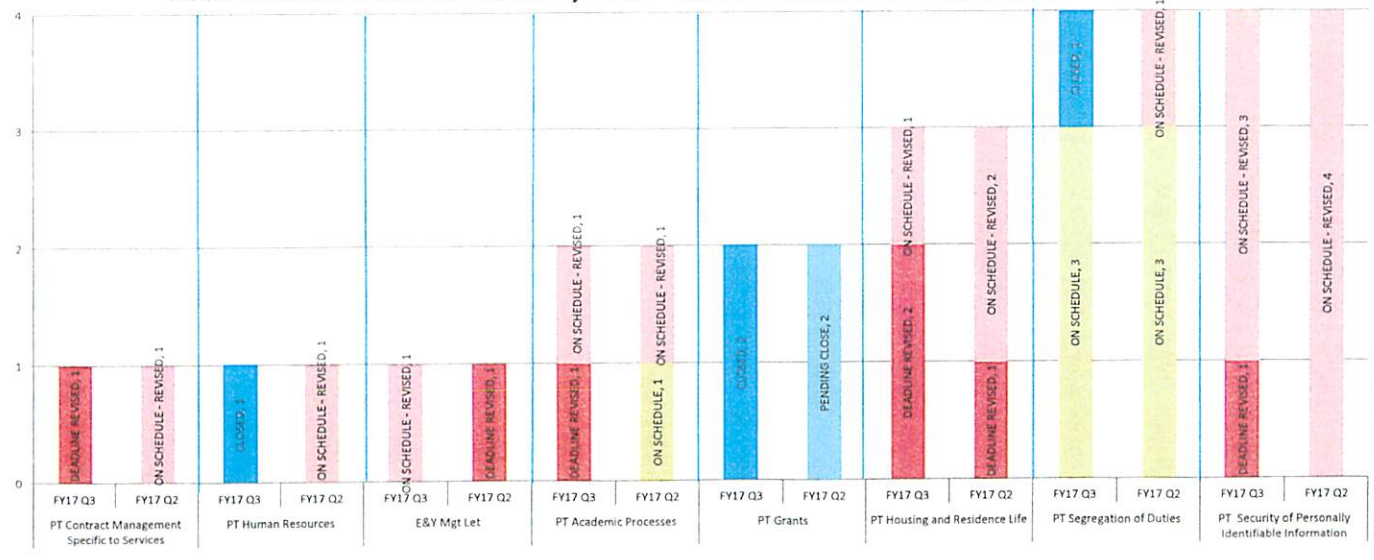
Risk Level



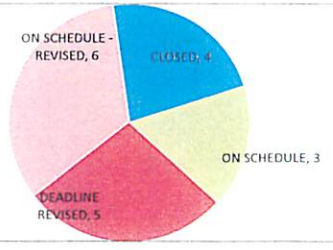
Risk Category



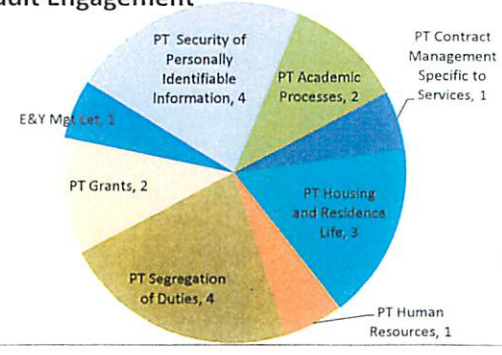
Audit Recommendations Status by Audit - Current Quarter vs. Prior Quarter



Status



Audit Engagement



prepared by: Sarah Gampo, Internal Audit
2/16/2017

AUDIT RECOMMENDATIONS STATUS - FY2017 Q3

Audit Recommendation Number / Name Audit Date Issued Risk Category Risk Level Division Original Deadline *Revised Deadline* Current Status	Summary of Recommendation	Summary of Response	Current Status Comment	Prior Status Comment
2007-01-0 DR Plan E&Y Mgt Let Oct. 2007 Information Technology Moderate Finance and Business Operations 9/30/2016 *6/30/2017* ON SCHEDULE - REVISED	The University should review the draft DRP plan to ensure it meets requirements in the event of a disaster. It should be tested to ensure that it functions as intended, includes a continuity strategy based on University priorities, and encompasses all key processes. A Business Impact Analysis (BIA) should be performed to determine the functions that are considered essential to the University's core business operations and the timeframe that these need to be recovered. Annually and when major changes occur to the technology environment, the plan should be reviewed, revised, and tested. [This recommendation was made in prior years.]	Several steps have been taken to address this repeated language to prepare the campus to move forward with the disaster recovery initiative. It is estimated that a complete and verifiable Banner-specific disaster recovery strategy will be delivered within 6-12 months following the implementation of the SCT Banner systems. In preparation for the Banner specific disaster recovery initiative, a service level agreement with Ohio State University to serve as YSU's disaster recovery site has been completed. Hardware was purchased to establish connectivity with Ohio State University. YSU personnel traveled to Columbus to install the hardware and have begun testing connectivity to YSU.	Three options were assessed for the DR strategy. The most cost effective option is to move all production computing resources to the new, but smaller server room in WCBA while incorporating the Main Distribution Frame (MDF) in Meshel Hall and another server room in Melnick Hall to mitigate risk. As a second phase of this DR initiative, slated for FY18, we will relocate our third copy of electronic data from Melnick Hall to an off-site location (either leveraging our reciprocity agreement with Akron University or to the SOCC) to mitigate a campus-wide disaster event.	The University of Akron DR site will not be implemented at this time. Ensuring the reliability of data center operations is the current priority, ITS is evaluating migrating the production computing environment to the State of Ohio Computing Center (SOCC) to leverage the state's resources. If the decision is made to migrate the production environment to SOCC, the existing data center will be used as the DR Site. The SOCC site visit is scheduled for 10/28/16 a decision is expected to be made by calendar year end. Deadline Revised to 6/30/17.
2012-01-0 New Hire Orientation PT Human Resources Feb. 2012 Human Resources Low Legal 7/31/2016 *12/31/2016* CLOSED	The Department of Human Resources should be responsible for processing all new hires and should orient all new employees to help ensure that University policies and procedures are properly communicated to new employees.	We agree that all newly hired University employees with the exception of student employees should be processed by Human Resources. The Manager, HRIS will be charged with researching ways to initiate and implement workflows to expedite the hiring process. Human Resources will collaborate with the Provost's Office to formulate and implement a part-time Faculty orientation program.	Electronic hiring process implemented 11/1/16.	Going live with electronic hiring process through PeopleAdmin on Nov 1, 2016. Part-time faculty orientation has been implemented.
2014-01-0 YSURF Financial Controls PT Grants Jan. 2014 Research Low Academic Affairs 6/30/2016 *10/31/2016* CLOSED	Currently, all accounting and operating functions are conducted by one individual. At a minimum, the bank statement should be reconciled by someone other than the sole YSURF staff and invoices should be approved by the YSURF staff's supervisor.	The YSURF President will bring the recommendation to the attention of the YSURF Board and will provide a follow-up response to the University.	Key financial controls currently in place include dual signature requirement on all checks and YSURF Board review of annual financial reports and banking activity.	YSURF has established banking services with PNC as of 9/22/16. "Two signature" new checks are forthcoming, and this will be the standard YSURF process going forward. A full financial audit has not yet been completed and will extend beyond October 31.

Audit Recommendation Number / Name Audit Date Issued Risk Category Risk Level Division Original Deadline *Revised Deadline* Current Status	Summary of Recommendation	Summary of Response	Current Status Comment	Prior Status Comment
2014-01-0 YSURF Strategic Direction PT Grants Jan. 2014 Research Low Academic Affairs 6/30/2016 ***10/31/2016*** CLOSED	We suggest that management consider developing a specific strategic direction for the YSURF and communicating it to employees.	The YSURF President and Board will work with University leadership (President, Provost, and Associate Provost and Dean of Graduate Studies and Research) to clarify the strategic direction and operation of YSURF.	Mission and strategies have been developed and documented. YSURF Board also meeting at least annually and documented meeting minutes are maintained.	Both Mission and High Level YSURF Strategies have been identified and will be presented to the YSURF Board at the next meeting. YSURF Mission and Strategies were presented to President Tressel and Staff on 9/14/16.
2014-02-0 Payroll Time Entries PT Segregation of Duties Apr. 2014 Financial High Finance and Business Operations, Legal 1/31/2016 ***9/30/2017*** ON SCHEDULE	There is a lack of segregation of duties for manual payroll time entries. There are employees who have the ability to enter manual time entries without additional approval or verification. This lack of segregation of duties increases the risk that incorrect or fraudulent paychecks may be issued. Manual time entries should be tracked and an individual should be assigned to confirm the validity of all manual time entries. This individual should not have access to create a manual time entry.	The Payroll Department, based on approved source documentation, is responsible to enter hours/time for the minority of hourly timesheets that were not electronically processed through self-service Banner. As a compensating control, a report will be developed to identify any hours manually entered. This report will be compared to the source documents by a different individual than the individual entering from the source document. Also, the Banner HR/Payroll security role classes were reviewed and the number of individuals with both duties has been reduced and segregated.	No change from previous status - System constraints include lack of a two-step process for processing payroll adjustments after the supervisor approval and lack of an audit trail for any changes made after the supervisor approval. Banner XE includes enhancements that are anticipated to reduce risk of improper adjustments being made without detection. However, due to unanticipated factors, including employee turnover and competing priorities in the IT area, this upgrade is currently not scheduled to be implemented until at the earliest the second quarter of 2017. Some compensating controls currently in place include the distribution of personnel reports after each pay to the Financial Managers, audit reports generated from the system to identify irregularities, and external audit procedures performed on payroll.	No change in status from prior comment.
2014-02-0 Payroll Processing PT Segregation of Duties Apr. 2014 Financial Moderate Finance and Business Operations, Legal 12/31/2015 ***9/30/2017*** ON SCHEDULE	There are 4 individuals with the ability to process/calculate payroll. Of these individuals, they all have ability to generate paychecks and add/approve hours, and 3 have access to record payroll in the general ledger and the ability to make general ledger entries. This lack of segregation within the process of generating the payroll creates and increases risk of error or fraud within a paycheck or payroll. We recommend a review of the workflow steps from running (calculating) the payroll through the financial recording of the payroll and reassign rights in the system to maximize segregation of duties.	Security access has been redesigned to limit the ability to perform the above workflow to only the Associate Controller. These functions are necessary for the Associate Controller in order to supervise the Payroll Department as well as the general accounting functions in the Controller's Office. However, any manual entry of hours by the Associate Controller will be reviewed in the audit report mentioned in Management's Response to Audit Finding & Recommendation #2. The security access for all of the other individuals mentioned has been segregated between entering, processing payroll, generating checks, and posting to the ledger.	No change from previous status - System constraints include lack of a two-step process for processing payroll adjustments after the supervisor approval and lack of an audit trail for any changes made after the supervisor approval. Banner XE includes enhancements that are anticipated to reduce risk of improper adjustments being made without detection. However, due to unanticipated factors, including employee turnover and competing priorities in the IT area, this upgrade is currently not scheduled to be implemented until at the earliest the second quarter of 2017. Some compensating controls currently in place include the distribution of personnel reports after each pay to the Financial Managers, audit reports generated from the system to identify irregularities, and external audit procedures performed on payroll.	No change in status from prior comment.
2014-02-0 Manual Payroll Checks PT Segregation of Duties Apr. 2014 Human Resources Moderate Finance and Business Operations, Legal 12/31/2015 ***9/30/2017*** ON SCHEDULE	There is a lack of segregation of duties with the manual (off-cycle) check process. There are individuals who can print manual checks and who have access to the check stock. An individual who has the ability to generate a manual (off-cycle) check should not have access to the check stock.	In order to segregate duties, the individuals who had access to the blank check stock no longer have the ability to initiate a manual check except for one person. As a compensating control, any manual entry of hours by that person will be reviewed in the audit report mentioned in Management's Response to Audit Finding & Recommendation #2.	No change from previous status - System constraints include lack of a two-step process for processing payroll adjustments after the supervisor approval and lack of an audit trail for any changes made after the supervisor approval. Banner XE includes enhancements that are anticipated to reduce risk of improper adjustments being made without detection. However, due to unanticipated factors, including employee turnover and competing priorities in the IT area, this upgrade is currently not scheduled to be implemented until at the earliest the second quarter of 2017. Some compensating controls currently in place include the distribution of personnel reports after each pay to the Financial Managers, audit reports generated from the system to identify irregularities, and external audit procedures performed on payroll.	No change in status from prior comment.

Audit Recommendation Number / Name Audit Date Issued Risk Category Risk Level Division Original Deadline *Revised Deadline* Current Status	Summary of Recommendation	Summary of Response	Current Status Comment	Prior Status Comment
2014-02-0 Employee File Changes PT Segregation of Duties Apr. 2014 Financial Moderate Finance and Business Operations, Legal 9/30/2016 ***12/31/2016*** CLOSED	There is a lack of segregation of duties within the process of entering and/or modifying the permanent employee file, which includes payroll and benefit information. This increases the risk of errors or fraudulent activity regarding the set up and payment of an employee. We recommend that an individual be assigned to verify that all additions and changes to the employee master file are authorized. This individual should not have access to make entries into the employee master file.	The Employee Processing Center (EPC) in the Human Resource (HR) department is responsible to enter employee information into the Banner employee master file based on approved source documentation. The Banner system cannot separate the ability to update the master file and the ability to approve changes to the master file, nor is it feasible to have and employee review all changes. HR is however in the process of implementing an electronic workflow to segregate these functions with expected implementation commencing December 2014. Currently, as a compensating control in addition to the new hire report, the EPC Manager will continue to review exception reports to identify irregularities and incomplete data. In addition, the number of employees with access to the master file has been reduced.	Electronic hiring process implemented 11/1/16.	Going live with electronic hiring process through PeopleAdmin on Nov 1, 2016. The new process kicks off an EPAF.
2015-01-0 SOC Reports PT Contract Management Specific to Services Oct. 2014 Information Technology Moderate Finance and Business Operations 10/31/2015 ***3/1/2017*** DEADLINE REVISED	There is no evidence that the University has a process in place to perform due diligence prior to contract execution to verify that a vendor has effective internal controls surrounding data confidentiality and security, when applicable. We recommend implementing a procedure to obtain and review Service Organization control Reports (SOC) to evaluate the suitability of the design and operating effectiveness of a service organization's internal controls relative to the service being provided.	A procedure will be implemented to require that service organizations provide a SOC report prior to contract execution and that periodic SOC reports are provided throughout the contract period. Agreement templates for the Standard Independent Contractor Agreement (SICA) and the Professional Service Agreement (PSA) will be updated to incorporate language to require SOC reports when appropriate. In addition, as part of Contract Administration, a procedure will be implemented to ensure that the University sponsor of the agreement has a procedure in place to obtain, review and file SOC reports with Procurement Services. An inventory of existing goods and service contracts will be performed to identify contracts which may be subject to SOC reports and efforts made to obtain and review such reports.	The list of vendors potentially subject to SOC reporting has been reviewed by Procurement Services and IT. Vendors were identified that require additional information for IT to make a determination of SOC reporting requirements. A SOC reporting checklist was created by IT and is currently being sent to contract sponsors (financial managers) to obtain additional information for IT to perform a risk assessment on prior purchases. For new contracts an electronic Security Review Form developed by IT is being created in eCUBE which will automatically route to IT Security Services to aid in the identification of the applicability of SOC reporting and assist IT in performing a risk assessment prior to contract execution. The new Security Review Form should be available for use by March 1st, 2017. Continued monitoring will consist of IT's on going monitoring of SOC reports, SOC requirements and risk assessments.	A list of current vendors that could potentially be subject to SOC reporting has been generated. From this list, Procurement Services will obtain information from the contract sponsors (financial managers) to assist IT in the determination of SOC reporting requirements. If SOC reporting is determined to be applicable, IT will contact the vendor to determine the availability of a SOC II report and then perform a risk assesment. Depending on volume, the deadline may need to be extended to perform a more thorough risk assessment. Continued monitoring will consist of IT's on going monitoring of SOC reports, SOC requirements and risk assessment. In addition, Procurement Services will implement a checklist developed by IT that will aid contract sponsors in the identification of the applicability of SOC reporting for new contracts so that a risk assessment can be performed by IT prior to contract execution.
2015-02-0 Locating PII PT Security of Personally Identifiable Information Nov. 2014 Information Technology High Finance and Business Operations 3/31/2016 ***1/31/2018*** ON SCHEDULE - REVISED	As part of the risk assessment process, the data classification policy in the University's "Sensitive Information Policy should be implemented. Highly sensitive PII data should be located in the processes and data system and evaluated for additional cybersecurity protection measures.	Network and Data security is in the process of evaluating areas known to utilize PII as well as the storage and accessibility of such data on a department by department basis.	On schedule as per prior quarter comment. Refer to status update presented by Associate Director of Network Security and Information Security Officer, Chris Wentz.	ITS is evaluating a software that will initially identify and locate sensitive data. Once the data is located, the systems and servers will be encrypted. The software will then scan for potentially senstitive data on an on-going basis in real-time; an employee in ITS will receive notification for review and follow-up.
2015-02-0 IS Audit Logs PT Security of Personally Identifiable Information Nov. 2014 Information Technology Moderate Finance and Business Operations 3/31/2016 ***5/1/2017*** DEADLINE REVISED	Audit logs are not routinely reviewed for potential security incidents or breaches. The University should consider using tools to create automatic reports from system activity logs that would identify system anomalies. These exception reports would be sent to IT personnel for investigation and timely follow up.	The University agrees. However, ITS must first implement a central log file repository and retain system logs for a consistent length of time. Once that is achieved, routine scanning of all logs will be explored. Packages that exist for this purpose will be evaluated at that time.	An Information Security Engineer position will be responsible for developing and monitoring alerts from system logs. Refer to status update presented by Associate Director of Network Security and Information Security Officer, Chris Wentz.	System logs are being retained in a central log file repository. The university already has software to scan the logs. ITS must develop "flags" for unexpected activity that the software will scan for and cause to trigger an alert. An employee in ITS will receive notification of alerts for review and follow-up.

Audit Recommendation Number / Name Audit Date Issued Risk Category Risk Level Division Original Deadline *Revised Deadline* Current Status	Summary of Recommendation	Summary of Response	Current Status Comment	Prior Status Comment
2015-02-0 Unauthorized Software/Hardware PT Security of Personally Identifiable Information Nov. 2014 Information Technology Low Finance and Business Operations 3/31/2016 ***1/31/2018*** ON SCHEDULE - REVISED	A list of authorized hardware and software should be complied. The University should employ scanning tools that will periodically scan the network for unauthorized software and devices and create action alerts.	YSU has deployed the Altiris Desktop management system. Not only does it push software, it inventories almost all software packages installed by users with administrator accounts. In addition, Altiris inventories authorized hardware connected to the wired network. YSU is exploring solutions that will identify and send an alert when unauthorized hardware is connected to the wired network.	On schedule as per prior quarter comment. Refer to status update presented by Associate Director of Network Security and Information Security Officer, Chris Wentz.	The implementation of Altiris is in process. Alerts when unauthorized hardware is connected to wi-fi are not deemed effective; alerts would only notify that unauthorized hardware connected, but could not identify the exact location and hence would not be actionable. ITS focus in identifying and protecting sensitive data -see related comment above on locating potentially sensitive data.
2015-02-0 USB Drives PT Security of Personally Identifiable Information Nov. 2014 Information Technology Low Finance and Business Operations 3/31/2016 ***1/31/2018*** ON SCHEDULE - REVISED	The University could configure the system to prohibit the copying of sensitive data onto USB drives, once the highly sensitive data has been identified in the system. In the event that there is a legitimate business need to use a USB drive, the University could configure the system to encrypt sensitive data when copied, or supply selected employees with hardware encrypted USB flash drives for use when copying PII.	The University will review its policies & procedures with regard to extracting PII to any mobile media or local storage in light of improved access restrictions being implemented. This review will include consideration of scanning local storage for PII as we believe PII stored locally poses a more significant security threat than mobile storage.	On schedule as per prior quarter comment. Refer to status update presented by Associate Director of Network Security and Information Security Officer, Chris Wentz.	Configuring systems to prohibit copying of data to USB drives will be considered for areas that routinely process large amounts of PII. ITS will have the ability to idenityf those areas once the system is in place to identify and locate potential PII noted in the related comment above.
2015-03-0 PT Faculty Contracts PT Academic Processes Feb. 2015 Human Resources Low Academic Affairs, Legal 7/31/2016 ***6/1/2017*** ON SCHEDULE - REVISED	We recommend that part time faculty contracts be electronically generated through the Human Resource system, and the contract routed electronically to the applicable people for electronic signature.	Human resources personnel are working to implement PeopleAdmin for generating part-time faculty contracts. This process is not simple as it requires the integration of two separate tracking systems; on to pull data from the personnel system and the other to integrate with the student registration system.	Parallel testing through PeopleAdmin continues. After testing is complete, a paperless hiring process will be rolled out. Part-time faculty orientation has been implemented.	We are currently working on a workflow through PeopleAdmin for Part-time faculty. Deadline Revised 6/1/2017.
2015-03-0 Tracking Faculty Workload PT Academic Processes Feb. 2015 Financial Low Academic Affairs, Legal 12/31/2016 ***12/31/2017*** DEADLINE REVISED	We recommend that further research be done to determine if the Banner System has the capability to calculate and track teaching hours, non-teaching time, and total faculty workload, and if the system does, then the use of the system should be implemented.	Banner has the ability to monitor faculty workload, and there is faculty workload non-teaching capability. A more detailed analysis of Banner system capabilities should be completed. The academic division is currently working with the Registrar's office to implement a full year scheduling and registration system; this system will make much of the data available at an earlier time and improve tracking and reporting processes.	We continue to await implementation of Banner XE. Implementation cannot occur without this critical system upgrade.	No change in status from prior comment.

Audit Recommendation Number / Name Audit Date Issued Risk Category Risk Level Division Original Deadline *Revised Deadline* Current Status	Summary of Recommendation	Summary of Response	Current Status Comment	Prior Status Comment
2016-02-0 Swipe Card System PT Housing and Residence Life Oct. 2015 Risk & Safety Low Student Experience 6/30/2016 ***8/1/2017*** ON SCHEDULE - REVISED	We recommend management consider a swipe card system, similar to that utilized by the University Courtyard apartments, for each of the student housing complexes.	Housing & Residence Life has already identified this as a need and has begun research on products and received preliminary quotes to determine approximate cost of the project. Plans are to move forward by the end of fiscal year 2016.	A committee has been formed that is currently reviewing 5 potential vendors for a swipe card system that will be in place in various locations on campus, including residence halls. Housing & Residence Life is targeting the Fall 2017 semester to have a swipe card system in place on residence halls. However, the implementation date is contingent upon when the swipe card system is implemented across the various locations on campus.	No change in status from prior comment.
2016-02-0 Background Checks PT Housing and Residence Life Oct 2015 Risk & Safety Low Student Experience 5/31/2016 ***3/15/2017*** DEADLINE REVISED	We recommend that criminal background checks be performed on all applicants for student housing. Furthermore, management should consider incorporating an application fee to the process to assist in offsetting such cost.	Housing & Residence Life will consider this recommendation. We will research potential vendors and costs associated with enough time to make a final decision for academic year 2016-2017 before the start of fall semester recruitment which begins on February 1, 2016.	Vendor agreement is in place and background checks will be performed on all applicants for student housing for the Fall 2017 semester.	As of 10/13/16, the vendor has not yet signed the contract. However, the background checks will be implemented by the end of Fall semester. Deadline revised to 12/1/16.
2016-02-0 Non-University Housing Options PT Housing and Residence Life Oct. 2015 Risk & Safety Low Student Experience 4/30/2016 ***5/1/2017*** DEADLINE REVISED	There are a number of housing options listed on the University website which appear to be endorsed by the University, yet not owned or managed by the University. We recommend management consider the feasibility of an affiliation, or referral agreement with the housing options not owned or managed by the Office of Housing and Residence Life.	We agree this could be a potential issue and will move forward with pursuing more formal affiliations with student housing facilities near and adjacent to campus.	The residential agreements have not yet been finalized and signed. The draft agreements are currently being reviewed by the General Counsel office.	No change in status from prior comment.

Youngstown State University
Office of Internal Audit
Audit Plan Quarterly Update
Fiscal Year 2017

	Quarter 2*			Quarter 3	Quarter 4	
	Actual	*Budget*	Difference	*Budget*	*Budget*	Comments
Audit and Assurance:						
Audit Engagements:						
YSUF Agreement	126	*96*	-30	*55*	*15*	report expected to be issued in Q4
Compliance	6.5	*70*	63.5	*0*	*0*	removed from audit plan to avoid duplication of efforts; majority of time re-allocated to Continuous Auditing/Analytics (see corresponding comment)
Purchasing		*0*	0	*105*	*145*	
Grants		*0*	0	*0*	*95*	audit will carryover to FY18 audit plan
Continuous Auditing/Analytics	20.5	*10*	-10.5	*200*	*100*	additional time allocated in Q3 to build sustainable analytic program based on best practice that leverage data to increase the depth and breadth of audit coverage [related IIA practice guides *Continuous Assurance* and *Data Analysis Technology*]; Q1 analytics completed in Q3 and report expected in Q4; Q2 analytics planned for Q3
Open Audit Recommendation Follow-up	12	*4*	-8	*30*	*20*	Q3 includes development of audit recommendation tracking database [related IIA standard *2500 Monitoring Progress*]
Hotline Monitoring	0	*0*	0	*15*	*15*	
	165	***180***	**15**	***405***	***390***	
Administrative & Planning:						
Administrative	63	*39*	-24	*36*	*26*	
Audit Risk Assessment, Annual Planning, Audit Subcommitte Prep and Meetings	34	*36*	2	*36*	*80*	additional time allocated in Q4 to enhance annual audit risk assessment with assurance mapping to ensure against duplication of efforts and coordination with other assurance providers [related IIA standard *2050 Coordination and Reliance* and practice advisory *2050-2 Assuarance Maps*]
Professional Development & Training	18	*25*	7	*11*	*4*	Q2 includes Ohio College and University Auditors semi-annual meeting; Northeast Ohio Institute of Internal Auditors Conference
Holiday, Vacation/Sick	72	*72*	0	*32*	*20*	
	187	***172***	**-15**	***115***	***130***	
Total Hours	**352**	***352***	**0**	***520***	***520***	

*actual and budget are for partial 2nd quarter beginning 11/1/16

prepared: 2/10/2017

Audit Timeline Matrix and Cybersecurity Update

IT Security Services

Audit Subcommittee

March 15, 2017

Christopher Wentz
February 10, 2017

Cybersecurity continues to cause unease for many public and private institutions. Higher Education has noted this global concern and for the second year, Educause has identified Cybersecurity as the number one IT issue facing universities. This finding, based on a survey sent to over 300 schools highlights the concern facing student success. As Youngstown State University continues to expand programs, research endeavors, and services to the campus and the global community, it is increasingly exposed to the potential threat faced globally by all individuals connected in the electronic ecosystem of computer servers and devices. As evidenced by the following, Youngstown State faces a global digital threat.

- In January 2017, only 21% of all email delivered to @ysu.edu email address was delivered to a user's inbox. This percentage includes advertisements and subscriptions such as newsletters. The remaining 79% was determined to be malicious or originated from a criminally controlled system.
- During the week of February 5th , over 65,500 attempted connection attempts or remote execution attempts cauterized as high or critical were blocked on University firewalls from over 50 individual countries including Russia, China, Iran, Kazakhstan, and the United States.

The threat environment facing Youngstown State is also constantly evolving and changing. Introducing new technology also presents new attack surfaces for malicious actors to exploit. Additionally, legacy devices and software are under constant review and attack by those same malicious actors looking to discover or exploit unknown or zero day vulnerabilities that exist within the environment. As this threat environment continues to evolve the development of the information security posture at Youngstown State is also set to develop.

Outlined below you will find expanded updates to the audit items covered in the Audit Matrix specific to IT Security Services. Internal Audit has been informed and involved in the review and selection of solutions being implemented to address recommendations. Input from those reviews between IT Security Services and Internal Audit was considered and incorporated in the selection and proposed deployment of the control. This update also includes the current state of a number of high-level goals and completed efforts.

Audit Recommendation 2015-02-01

In an effort to address the identification of sensitive information within University systems, the IT Security Services Department has selected and is currently working with the Procurement Services Department to secure software. This software, designed to identify sensitive information and report on the creation or movement of the data will assign a cyber dollar and risk value to the individual record. Based on this value, systems that hold the most significant risk can be identified and appropriate measures can be taken to secure the asset and data. Systems with higher values will be prioritized for review and remediation.

Audit Recommendation 2015-02-02

Currently IT Security Services is functionally testing software that will allow the correlation of logs from servers and network devices. This solution will allow 90 days of retention for immediate review and retrieval. Additional storage can be secured and provide unlimited retention if necessary. The service allows IT Security Services to establish parameters for alerts and provide feedback to a centralized dashboard. As a Security Engineer position is added, the review of these logs will become a daily activity. This software is currently in the procurement process and timely acquisition is expected. Once deployed, the system and review procedure will be evaluated by Internal Audit for modifications and compliance to the audit recommendation.

Audit Recommendation 2015-02-03

IT Security Services has met with Internal Audit in addition to supporting departments to discuss the ability to inventory software and hardware. Currently, software is managed using the Altiris Desktop Management System. While this addresses one component of the audit recommendation, the second specific to network devices is still under development. The University is currently underway with a network refresh that will replace a number of legacy devices and may provide the opportunity for more options of identification of rogue devices using a network access control. However, prior to the full deployment of this network refresh IT Security Services will begin to scan and review at regular intervals the network for unknown or unregistered devices. This regular scan will be reviewed by Internal Audit for compliance to the audit recommendation.

Audit Recommendation 2015-02-04

As mentioned in Audit Recommendation 2015-02-01, software will be introduced to inventory sensitive data. The recommendation suggests the possibility of configuring a system to limit USB functionality. While this is one solution to potential data loss, it does not address the entire concern of sensitive data movement and maintaining functionality for the end user. The first concern is addressed with the chosen software by providing real-time indexing of sensitive information and reporting on the location of the data. Providing information on use, creation and location allows IT Security Services to identify areas of concern as well as areas of high concentration. It also provides intelligence on data being shared or duplicated to cloud storage. This would be overlooked if addressing USB storage alone. Secondly it maintains functionality of drives for end users who rely on USB storage to preform job duties independent of interaction with sensitive data.

It is also notable that IT Security Services has a Committee within the newly established IT Governance model. This committee, the Security and Policy Advisory Committee (S-PAC) will address security and policy related items affecting the campus community. This group consists of individuals from various campus departments including CSIS, General Council, YSU Police, Procurement Services, Internal Audit, IT, and student representation. The group aims to educate the campus, refine University policies, and provide guidance for information security related technology.

Additionally, the IT Security Services is currently developing a vulnerability management program. This program looks to address the regular scanning of systems and network hardware for vulnerabilities. This software will also be leveraged against new systems prior to deployment into production. If issues are found, this program will track remediation efforts and retesting to validate corrective measures are effective.

Lastly, IT Security Services is currently deploying enhanced email protection expanding coverage to all @ysu.edu email addresses. Previously, some protection mechanisms were only effective if the individual was connected to the University network. With this enhancement, the user will be protected from malicious links and attachments wherever they chose to access email. This includes mobile devices and home computers.

High Level Efforts

Completed

Selection of tool to help identify highly sensitive Personably Identifiable Information (PII).

Selection of tool for vulnerability management program.

Selection of tool for log correlation, alert management, and retention.

Enhanced email protection.

Strengthened firewall filtering rules and alerts.

In Progress

Implementation of sensitive data location and risk tool.

Implementation of vulnerability management software and program.

Identification of servers, systems, and network devices to incorporate into logging system.

Expansion of email protection to all @ysu.edu email addresses.

Physical and logical separation between various departments and resources.

Onboarding of student and full time employee.

Current Year Goal

Enhanced email protection to all @student.ysu.edu email addresses.

Promote education and awareness to campus community.

Align strategically to industry cybersecurity framework, Higher Education Information Security Council (HEISC).

Establish tools and procedures to gain better visibility into network activity.

Review, revise, and recommend changes to applicable policies and procedures within IT Security Services.

Further refine boarder firewall rules to address repeated or emerging threats in addition to align with industry best practices.

Respectfully Submitted,

Christopher Wentz
Information Security Officer
Youngstown State University

Youngstown
STATE UNIVERSITY

RESOLUTION TO MODIFY THE NAME OF THE OFFICE OF INTERNAL AUDIT AND RISK MANAGEMENT

WHEREAS, the internal audit activity is performed by the Office of Internal Audit and Risk Management; and

WHEREAS, the Internal Audit Charter (the Charter) approved by the Audit Subcommittee on November 30, 2016 defines the internal audit activity's purpose, authority, and responsibility; and

WHEREAS, the Charter states that internal auditing is an independent and objective assurance and consulting activity designed "to evaluate and improve the effectiveness of the University's governance, risk management, and internal control"; and

WHEREAS, risk management is the process of making decisions to manage and mitigate uncertainties, including transfer of risk through insurance; and

WHEREAS, performing risk management functions would impair the independence and objectivity of the internal audit activity when evaluating the effectiveness of risk management; and

WHEREAS, the Office of Internal Audit and Risk Management does not perform risk management functions; and

WHEREAS, the name of the "Office of Internal Audit and Risk Management" has been modified to the "Office of Internal Audit" to appropriately reflect its function and ensure the independence and objectivity of the internal audit activity.

NOW, THEREFORE, BE IT RESOLVED, that the Board of Trustees of Youngstown State University does hereby acknowledge the modification of the name of the Office and Internal Audit and Risk Management to the Office of Internal Audit.

Board of Trustees Meeting
March 16, 2017
YR 2017-