University of Houston Information Technology

Line	Internal Audit Report No.	Action No.	Action Manager	Current Complet. Date	Status	Action To Be Taken	Status Description
1	SAO Report #05-010	16	McGee, Jim	12/17/2004	**Complete**	Conduct a review of all stale accounts and disable and remove accounts, as necessary.	**Action Complete**. A review of accounts was conducted to identify accounts that were stale or belonged to individuals no longer associated with the University. These accounts were disabled and effectively removed and, therefore, no longer pose a security risk.
2	SAO Report #05-010	1	Jain, Arun	1/31/2005	**Complete**	Review separation of database administrator (DBA) duties and implement changes to ensure that DBAs do not have access to security functions and other applications. Where separation of duties is not practical, appropriate supervisory reviews will be implemented	**Action Complete**. Enterprise Systems has initiated seperation of duties and monthly supervisory reviews of both High Level accounts (Oracle/DBA) and Security Roles for HR/Payroll System. Reviews include access control and documentation (See attached polic
3	AR 2005-08	1	Spindler, Bill	2/28/2005	**Complete**	Meet with customers to discuss needs, projects and overal performance to help better align CTS with its customer base	**Action Complete** for Audit requirements; expanded to all IT Departments for incorporation into best practices.
4	SAO Report #05-010	6	Jain, Arun	3/31/2005	**Complete**	Identify critical data in the HR/Payroll and Student systems and establish additional procedures, as necessary, to review changes.	**Action Complete.** HR/Payroll has processes in practice to review, audit critical data changes (Marli Bober). Enrollment Services has processes in practice to review, audit critical data changes (Ed Apodaca).
5	AR 2005-08	3	Spindler, Bill	6/30/2005	**Complete**	Develop position guides for all CTS positions to enhance the level of understanding of roles, reponsibilities and processes	**Action Complete**
6	SAO Report #05-010	2	Mazhar, Haseen	7/1/2005	**Complete**	Perform annual reviews of high-level user accounts to ensure that accounts are still necessary. **ACTION 1:** **ACTION 2:** **ACTION 3:**	**Submitted to Internal Audit Review.** Enrollment Services awaiting review by IA

University of Houston Information Technology

Line	Internal Audit Report No.	Action No.	Action Manager	Current Complet. Date	Status	Action To Be Taken	Status Description
7	SAO Report #05-010	3	Mazhar, Haseen	7/1/2005	**Complete**	Review and correct internal procedures to ensure that high-level users always have proper authorization documentation. **ACTION 1:** **ACTION 2:** **ACTION 3:**	**Partially implemented - Updated Management's Response:** The Enterprise Systems Department is working with functional users to review and correct internal procedures in their respective areas to ensure that high-level users always have proper authorization documentation. Expected completion date: July 1, 2005. (8/22/05 - Enrollment Services awaiting review by IA.)
8	SAO Report #05-010	15a	McGee, Jim	7/31/2005	**Complete**	Develop and implement procedures for disabling and removing accounts of users who leave the University or change jobs within the University. **ACTION TO COMPLETE: I/A WILL CONFIRM COMPLETION**	***Action Complete***
9	AR 2005-08	2	Beach, Fran	7/31/2005	**Complete**	Perform and document a security risk analysis and assessment of the university's information technology infrastructure under CTS' operations to help ensure it is protected against unauthorized access, loss, disclosure, modificaiton, disruption or destruct of information resources whether accidental or deliberate, in accordance with TAC § 202.	**Action Complete**
10	SAO Report #05-010	4	Jain, Arun	8/31/2005	**Complete**	Assess the sharing of user IDs and passwords among DBAs and develop an action plan for providing a fully auditable environment by individual.	**Action Complete**

University of Houston Information Technology

Line	Internal Audit Report No.	Action No.	Action Manager	Current Complet. Date	Status	Action To Be Taken	Status Description
11	SAO Report #05-010	10b	Chambers, Charles	10/31/2005 12/31/2005 05/31/2006 09/30/2006	**Partially Implemented**	Require all faculty, staff and student users of the authorized wireless network to authenticate their identities using a user ID and password. **ACTION 1:** Meet to discuss table and understand communication plan. **ACTION 2:** Publish new services **ACTION 3:** Review by CMC **(an incremental review is ongoing as each change is proposed)** **ACTION 4:** Submit documentation to I/A for review. CONTINUED BELOW	***Partially Implemented*** **- Updated Management's Response:** The new compliant Wireless service "UHWireless" is currently operational, but not communicated to campus for redirecting existing wireless users from the legacy wireless service. IT is preparing information for communication to campus as part of new fall 2006 semester. This will be completed and the legacy wireless service retired following the start of the fall semester, Sepember 14, 2006. Final completion date September 30, 2006.

University of Houston Information Technology

Line	Internal Audit Report No.	Action No.	Action Manager	Current Complet. Date	Status	Action To Be Taken	Status Description
11 cont	SAO Report #05-010	10b				**Steps to completion of the change-over are:** 1. Change wireless SSID from vendor default ("tsunami"). a. An alternate SSID ("UHWireless", termed UHWireless service) has been implemented for campus (using the same wireless infrastructure) and is be broadcasted with the existing legacy default SSID ("tsunami"). b. The default SSID "tsunami" will not be broadcasted after July 17, 2006. This still allows user to connect if they are already configured for the SSID, but new users would not see the old legacy default SSID (tsunami"). This allows a transition time period for existing users. c. IT/TSS will advertise the new UHWireless service as part of the start of the 2006 Fall Semester startup. The material will be finalized and published as part of IT's Cougar First Impression support. d. Signage will be posted in all current wireless coverage areas for the new UHWireless service during July/August. e. The old legacy SSID "tsunami" will be retired on Monday, September 14, 2006.	
12	SAO Report #05-010	11	Beach, Fran	8/31/2005	**Complete**	Ensure that all critical systems will only accept a campus LAN or other connections utilizing the VPN service. **ACTION TO COMPLETE: I/A WILL CONFIRM COMPLETION**	***Action Complete***
13	SAO Report #05-010	12a	Chambers, Charles	10/31/2005 05/31/2006	**Partially Implemented**	Rename all authorized wireless access points from the default SSID to a unique name. **Combined by I/A with 10a - see line number 11**	**Combined by I/A with 10a - see line number 11**

University of Houston Information Technology

Line	Internal Audit Report No.	Action No.	Action Manager	Current Complet. Date	Status	Action To Be Taken	Status Description
14	SAO Report #05-010	18a	McGee, Jim	01/02/2006 01/12/2006	**Complete**	Modify processes which preclude maintaining password history and implement CougarNet password history. Password standards (see line 24) include: Lockout: After 5 consecutive failed login attempts an account will be locked for 30 minutes. **ACTION 1:** Launch elements of Communication Plan per Plan **ACTION 2:** CMC Review **ACTION 3:** Submit final document to I/A (to include CMC approval and Com Plan completion) for I/A review and approval.	***Action Complete*** **- Updated Management's Response:** The Information Technology Department has enabled password history in CougarNet to help prevent users from reusing the same password and will raise the Passwords Remembered from 5 to the system maximimum of 24 on January 12, 2006 in order to further prevent the reuse of a password.
14 cont						*Extended Description necessary because text exceeds 225 characters*	Password history was implemented on CougarNet in August. This means that you cannot reuse your last four passwords for CougarNet. Password history will be included in information about password complexity because it will be convenient and because the history time interval will change. Password complexity has already been implemented for PeopleSoft systems Password complexity will be implemented for CougarNet and the other enterprise servers administered by IT in January. The password chosen has to meet certain basic requirements - see Action To Be Taken column. A document listing servers and password standards standards is under development. Manager will review the implementation deadline in regards to the holiday time frame.
15	SAO Report #05-010	19	Longoria, Sam	8/31/2005	**Complete**	Modify procedures to require a systematic test of the disaster recovery plan annually.	**Submitted to Internal Audit for review.** **Reported as Completed.**

University of Houston Information Technology

Line	Internal Audit Report No.	Action No.	Action Manager	Current Complet. Date	Status	Action To Be Taken	Status Description
16	SAO Report #05-010	21	Stevenson, Beverly	8/31/2005	**Complete**	Update the security program in order to incorporate the requirements of GLB, TAC 202, and other regulations and finalize policies and procedures for the University in regards to information security.	**Submitted to Internal Audit for review.** **Reported as Completed.**
17	SAO Report #05-010	22	Stevenson, Beverly	11/30/2005	**Complete**	Work with Technology Support Services in order to develop an information security awareness training program. **ACTION 1:** **ACTION 2:** **ACTION 3:**	**Partially implemented - Updated Management's Response:** The Information Security Awareness Training (ISAT) Program has been developed in WebCT and is being tested. Deployment to the University of Houston will occur not later than November 30, 2005. Legal has approved. Reported as Completed.
18	SAO Report #05-010	23	Longoria, Sam	8/31/2005	**Complete**	Establish a mechanism to ensure users' acknowledgment of responsibilities regarding their responsibility to comply with security requirements, and to determine how often this acknowledgment will be required to be renewed. **ACTION 1:** **ACTION 2:** **ACTION 3:**	**Submitted to Internal Audit for review.** **Reported as Completed.**
19	SAO Report #05-010	5	Longoria, Sam	8/31/2005	**Complete**	Begin a monthly review of the access logs for high-level user accounts to insure account integrity. **ACTION 3:** I/A must confirm acceptance	***Action Complete***

University of Houston Information Technology

Line	Internal Audit Report No.	Action No.	Action Manager	Current Complet. Date	Status	Action To Be Taken	Status Description
20	SAO Report #05-010	13	Longoria, Sam	8/31/2005	**Complete**	Establish a schedule to regularly scan the University network for vulnerabilities. **ACTION 1:** **ACTION 2:** **ACTION 3:**	**Submitted to Internal Audit for review.** **Reported as Completed.**
21	SAO Report #05-010	25b	Green, Steve	11/1/2005	**Complete**	The information security officer will report to the UH president on the status and effectiveness of the information resources security controls and on an annual basis thereafter. **ACTION 1:** Steve Green to review **ACTION 2:** Document & submit to I/A for review.	***Action Complete*** - Updated Management's Response: The information security officer's report will be presented to the UH president in October 2005, and annually thereafter. Estimated completion date: November 1, 2005. Copy of report received.
22	SAO Report #05-010	8b	Mazhar, Haseen	12/31/2005 03/31/2006	**Complete**	Initiate a process to provide a transition in the Student System from FTP and Telnet to a secured environment, including disabling non-secure FTP and Telnet. **ACTION 1:** Document & submit to I/A for review by 03/15/06.	***Partially Implemented*** **- Updated Management's Response:** Telnet has been disabled on the Student System. The Student System is accessed through a secured encrypted connection (SSH). Secure FTP is being implemented for file transfer. However, non-secure FTP is available to some users. The target date for disabling non-secure FTP is March 31, 2006.
23	SAO Report #05-010	9	Mazhar, Haseen	12/31/2005	***Complete***	Implement software to encrypt Student System user IDs and passwords. **ACTION 1:** I/A is in receipt of documentation - Waiting review by I/A.	***Action Complete*** to meet timeline. Documentation submitted. To be reviewed by Audit Group 12/12/05. Student System will go to PS, no PW changes until then.

University of Houston Information Technology

Line	Internal Audit Report No.	Action No.	Action Manager	Current Complet. Date	Status	Action To Be Taken	Status Description
24	SAO Report #05-010	17a	McGee, James (CougarNet and identified by I/A as Action Mgr) Martin, Keith (PeopleSoft)	1/2/2006 05/15/2006 12/31/2006 The final date will be driven by the readiness of the campus.	**IA Review Required**	**ACTION 1:** PS implementation of password standards occured 9/1/05. **ACTION 2:** Cougarnet scheduled to follow. **ACTION 3:** CMC Review. **ACTION 4:** Document & submit to I/A for review. Require passwords to be at least eight characters in length and that are composed of letters, numbers, and special characters.	**Partially Implemented: Updated Management's Response:** We are developing system risk profiles to assign the appropriate level of password complexity to various systems and expect the revised security policy to be implemented by December 31, 2006. **Notes: Implementation date subject to approval by Faculty Senate. The expanded scope enables IT to match password standards with risk level.**
25	SAO Report #05-010	24	Fouty, Dennis	12/31/2005	**Complete**	The information security officer will report to the appropriate level of management.	**Action complete**. We created a dotted line reporting relationship in which the institutional security officer reports to the chief information officer of UH. The information security officer maintains a solid line reporting relationship to the assistant vice president for Security and Disaster Recovery (SDR). We are evaluating the designation of the assistant vice president of SDR as the university's information security officer.
24 cont						*Extended Description necessary because text exceeds 225 characters* Password standards are: 1. Minimum Password Length: 8 characters 2. Prompt for New Password: every 90 days 3. Password History: 4 passwords – this is based off prompting for a new password every 90 days. Passwords in the history will not be available for reuse. 4. Require at least one character from each of the following classes: a. Alphabetic: Upper and Lower case (a-z, A-Z) b. Numeric: 0-9 c. Special Characters: ! # $ % & ( ) * @ ^ 5. Lockout: After 5 consecutive failed login attempts an account will be locked for 30 minutes.	Implemented Sept 1 - PeopleSoft, CougarNet, others in TSS to be verified Computer Passwords Standards document Submitted to Internal Audit for review. The specific points in the standard will be enforced by the servers as best they can on January 2. (Not all restrictions are supported on all servers.) Users will see the change through a 90-day window that starts on January 2. During that time we will be communicating good password practices and tips on making passwords secure and easy to remember. The Student System was included in this item, although not originally of concern. Haseen Muzhar and Keith Martin have responded. Password history was implemented on CougarNet in August. This means that you cannot reuse your last four passwords for CougarNet. Password history will be included in information about password complexity because it will be convenient and because the history time interval will change. Password complexity has already been implemented for PeopleSoft systems. Password complexity will be implemente

University of Houston Information Technology

Line	Internal Audit Report No.	Action No.	Action Manager	Current Complet. Date	Status	Action To Be Taken	Status Description
26	AR 2004 -01	2a	Vazquez, Daisy	12/31/2005	**Complete**	Work with the Purchasing Department to obtain competitive rates for mobile telephone sevices and establish process to periodically assess these rates. **ACTION 1:** Verify requirements of action item. **ACTION 2:** Document & submit to I/A for review and approval.	***Action Complete*** - In addition to recently implementing the new Federal Government General Services contract for services through Verizon providing strong competivtive rates to participants, we have solicited and received agressive discounts formulated on a University Program offering from Major Wireless Vendors covering Corporate, Individual and Student lines. Initiative will support the new employee stipend program being developed by Administration & Finance. Contract preparation and processing is underway with Sprint and Verizon with Cingular to follow. We anticipate to have all major vendor contracts in the processing mode by December 31, 2005. Thereafter review rate and plan structures with vendors annually.
27	SAO Report #05-010	7a	Mazhar, Haseen	12/31/2005	**Complete**	Work with external parties to help ensure that information is exchanged securely. **ACTION 1:** Document & submit to I/A for review and approval.	***Action Complete*** - The capability of exchanging information securely (using secure FTP or secure Shell) has been implemented. While four of the 14 interfaces are now being done with Secure FTP, we are still working with the remainder to ensure technical compatibility. This process will coincide with the process to provide a transition in the student system from FTP and Telnet to a secured environment. We expect this to be completed by December 31, 2005.

University of Houston Information Technology

Line	Internal Audit Report No.	Action No.	Action Manager	Current Complet. Date	Status	Action To Be Taken	Status Description
28	AR 2003-16	3e	Broyles, Nicole	02/28/2006 06/30/2006 12/15/2006	**Partially Implemented**	Develop a MAPP that delineates the responsibilities of divisions, colleges, and departments for the management and internal control of departmental information technology resources. **ACTION 1:** Final review all parties **ACTION 2:** Document & submit to I/A for review and approval.	Partially implemented -- IT developed MAPP 10.03.06 in FY 2004 and submitted it to the Office of Policies and Procedures for formal campus reviews, as well as taking it to additional campus committees such as the Dean's and Research Councils. All IT MAPPs were submitted to ITCC for review in May, 2006. Review of this MAPP by ITCC and Academic Affairs senior management is complete. However, per request from the Faculty Senate, no policies will be implemented during the summer months. The next policy 3-month cycle begins in August and concludes at the end of November.
29	SAO Report #05-010	14a	Glendinning, Phil	6/30/2006	**Complete**	Review the viability and resources required to expand internal network monitoring utilizing IDS tools and create an action plan. **ACTION 1:** Equipment to be installed **ACTION 2:** Document & submit to I/A for review and approval.	***Action Complete*** - SDR completed the review of expanding the internal network monitoring and created a recommended action plan. SDR will work with IT management to finalize and operationalize the action plan. Estimated completion: June 1, 2006. Equipment ordered.
30	SAO Financial Systems	1	Beach, Fran	10/28/2005	**Complete**	**Recommendation:** Limit access to the PeopleSoft Financial Application from the Internet. **Response:** As noted in the report, the University has disabled the Internet connection to the Financial System to further ensure the University's resources are not exposed to unauthorized access.	**Action completed.** Documentation has been provided to IA.

University of Houston Information Technology

Line	Internal Audit Report No.	Action No.	Action Manager	Current Complet. Date	Status	Action To Be Taken	Status Description
31	SAO Financial Systems 06 012	1	Block, Eric	6/30/2006 08/31/2006	**In Process**	**Recommendation:** The University should, as it implements both routers with firewall capabilities at the enterprise comupter center, migrate the PS servers behind the firewall with a properly configured firewall rule set. **Response:** The University will perform a risk assessment of the specific vulnerability that was communicated separately to improve the security of the Financial System by June 30, 2006. **ACTION 1:** Complete proposal with Charles Chambers and gain concurrence. **ACTION 2:** Document & submit to I/A for review and approval. **Prior Response w/ Additional Detail:** The University will perform a risk assessment of its network usage to be completed by June 30, 2006. The risk assessment will cover both internal and external usage of the financial enterprise architecture and the University will determine what additional architectural approaches, including both in	Partially Implemented: Updated Management Response: A risk assessment has been completed. IT will present it to Internal Audit for review. We will use the outcome to plan security improvements of the financial system as part of our Payment Card Industry (PCI) network improvement plan. Final completion date: August 31, 2006.
32	SAO Financial Systems	3	Glisson / Martin will advise / Chan will review logs			The University should design policies and procedures for monitoring the PSACCESS application log, regularly monitor the log, and follow up on any issues noted in the monitoring efforts.	Chan will review logs to determine patters if any to establish criteria, and identify tools and who will monitor. Martin to advise.

University of Houston Information Technology

Line	Internal Audit Report No.	Action No.	Action Manager	Current Complet. Date	Status	Action To Be Taken	Status Description
33	SAO Financial Systems	4	Chan / Martin			**Recommendation:** Improve effectiveness of manual user access controls. **Response:** We will develop procedures to identify and lock-out users that have not logged in for six months by November 30, 2005.	**In Process** **To Complete (IT Responsibility):** Finance may require CSR for additional work
34	SAO Financial Systems 06 012	5	Martin, Keith	3/31/2006	**In Process**	**Recommendation:** Determine the cause for the automated application security errors and correct them. **Response:** We have determined that six of the user accounts that were not automatically disabled related to users not changing their passwords after the had been reset. **ACTION 1: Verify acceptance by I/A**	**In Process** To Complete: documentation / report to IA I/A will be requested to review and verify.
35	SAO Financial Systems	6	Chan			**Response:** As noted in the report, we have disabled the default user account in the Financial System which was not disabled during installation of the Financial System.	**Action Complete** Finding changed
36	SAO Financial Systems	7	Chan			**Response:** The university will document descriptions of the security roles in the Financial System by March 31, 2005.	

University of Houston Information Technology

Line	Internal Audit Report No.	Action No.	Action Manager	Current Complet. Date	Status	Action To Be Taken	Status Description
37	SAO Financial Systems	8	Chan			**Response:** Access for the Director of Financial Systems will be modified, so that she cannot add, change, or delete financial transactions in the production database. Her access was modified November 1, 2005.	In Process
38	SAO Financial Systems 06 012	6	Block, Eric	3/31/2006	**Complete**	**Recommendation:** Ensure that the account with extensive database access is assigned to a specific individual, the password for the account is not shared, and the account is used only when a task requires the access that this account provides. **Response:** The University will assign an individual the responsibility of overseeing operational use of "extensive access" accounts. Access to the data using these accounts by individual database administrators is being logged, and an "individual usage" review process will be put in place by March 31, 2006. **ACTION 1:** Submit external process documentation to I/A for review and approval.	**In Process** To Complete: Assign individual / documentation of log review / report from Audit Team to Internal Audit as to completion Internal process has been reviewed and approved by I/A. External process must be submitted to I/A.

University of Houston Information Technology

Line	Internal Audit Report No.	Action No.	Action Manager	Current Complet. Date	Status	Action To Be Taken	Status Description
39	SAO Financial Systems 06 012	7	Block, Eric	3/31/2006	Complete	**Recommendation:** Ensure that the account with extensive database access is assigned to a specific individual, the password for this account is not shared, and the account is used only when a task requires the access that this account provides. **Response:** The University will include the review of individual direct database access from the network and from the database server in its normal review process by March 31, 2006. **ACTION 1:** Define accountability. **ACTION 2:** Document & submit to I/A for review and approval.	**In Process** To Complete: include Listener in normal review process / documentation / Report to Internal Audit Review process is complete.
40	SAO Financial Systems 06 012	8	Block, Eric / Green, Steve to advise	3/31/2006	Complete	**Recommendation**: The university should implement appropriate password controls that are similar to those described in the security policy for the financial system. These controls could include locking out user accounts after three failed log-in attempts and setting passwords to expire after 60 days. **Response**: We will implement appropriate password controls for database user accounts that are similar to those described in the security policy for the financial system, including locking out user accounts after three failed log-in attempts and setting passwords to expire after 60 days. The appropriate controls will be implemented by March 31, 2006. **ACTION 1:** Run in Test until 12/31/05 **ACTION 2:** CMC review. **ACTION 3:** Document & submit to I/A for review and approval.	**In Process** To Complete: documentation / Report to Internal Audit Implement the same password controls as used by Finance for databases. Elected to implement PeopleSoft standards.

University of Houston Information Technology

Line	Internal Audit Report No.	Action No.	Action Manager	Current Complet. Date	Status	Action To Be Taken	Status Description
41	SAO Financial Systems 06 012	12	Beach, Fran	In discussion with IA	**IA Review Required**	**Recommendation**: The university should store the copies of the file interity hashes on a write once/read-only CD/DVD in order to ensure that an attacker cannot alter the values. **Response**: As a matter of routine operations, starting in January 2002, the University has been copying the file integrity hashes on to tape in case the hashes residing on the server are compromised. **ACTION 1:** **ACTION 2:** **ACTION 3:**	**In Process** To Complete: documentation / Report to Internal Audit Documentation has been submitted to I/A: waiting for approval to complete.
42	SAO Financial Systems 06 012	9a	Block, Eric	03/31/2006 05/31/2006 07/31/2006	**IA Review Required**	**Recommendation**: The university should perform a risk assessment and cost/benefit analysis of enabling the auditing functions. The university should activate the appropriate auditing functionality in the Oracle database based on the results. **Prior Response**: The University will determine which tables should be captured with Oracle Auditing based on the risk associated with those tables. The assessment will be completed and implemented by March 31, 2006.	Partially Implemented: Updated Management Response: IT and the business owner have determined which tables should be captured. The capture of these mutually agreed tables has been implemented in production. IT will now obtain the business owner's cncurrence with the solution. Final completion date: July 31, 2006.

University of Houston Information Technology

Line	Internal Audit Report No.	Action No.	Action Manager	Current Complet. Date	Status	Action To Be Taken	Status Description
42 cont	SAO Financial Systems 06 012	9	Block, Eric	03/31/2006 05/31/2006	**IA Review Required**	**Response 04/12/06**: Oracle Auditing is turned on in Test, and audit information is being captured. We are working with end users in Finance to determine how the information will be used, what queries will be run against it, and what procedures they will use to review the data. Once the Finance area has determined their review process, we will turn Auditing on in Production. Anticipated date of implementation in Production is 05/31/06. **Abbreviated Response to BOR 5/2/06**: We are working with the Finance Department to determine which tables should be captured with Oracle Auditing and the procedures for reviewing this data. Estimated implementation date: May 31, 2006. ACTION 1: Risk assessment from end-user perspective. ACTION 2: Risk assessment from technical perspective. ACTION 3: Recommendation of action path based on risk assessments. ACTION 4: Document & submit to I/A for review and approval.	**Completed**. Based on Joint Technical and User review 43 PS tables where slected as canditates for Oracle Auditing. Auditing was turned on for these tables in test and run for a full month. Based on results Auditing was turned on in production on 5/28/2006. A complete documentation package was submitted to IA on 5/30/2006. Responce delayed due to IA workload. . . .
~~**43**~~	~~SAO Financial Systems~~	Dropped	~~Glisson~~		**Removed from Audit Findings**	~~The university should prevent users from changing the default numbering values unless vairation is properly limited, documented, and accounted for by the appropriate university staff.~~	~~UH does not agree as this is for reference not control. We need to list rules and determine what constitutes an exception and the interval for review of such reports.~~

University of Houston Information Technology

Line	Internal Audit Report No.	Action No.	Action Manager	Current Complet. Date	Status	Action To Be Taken	Status Description
44	SAO Financial Systems	13	Glisson			The University should make purchase coding information more available to the departments and provide effective training to individuals who make coding decisions. The University should also perform more effective review procedures to ensure that purchases are coded appropriately.	
45	SAO Financial Systems	15	Glisson			The university should ensure that the accounts payable balance at year-end materially reflects expenses incurred as of year-end that will not be paid until the subsequent period.	
46	SAO Financial Systems	16	Glisson			The University should perform a risk assessment to determine the cost/benefit of increasing the field capture in PSAUDIT. Increases should be made based upon the risks identified in the assessment.	
47	AR2006 25	1	Aycock, Mark Frankfort, David	8/31/2006	**In Process**	*Finding:* Significant weaknesses in internal controls over fixed assets in the data center. **ACTION 1**: Tag all untagged IT servers, hosted servers and remaining untagged assets, such as network elements and software. **ACTION 2**: Document & submit to I/A for review and approval.	Notes: This action should be used as an opportunity to refresh and revise our practices in IT. A review of State and UH policies for tagging software should be performed.

University of Houston Information Technology

Line	Internal Audit Report No.	Action No.	Action Manager	Current Complet. Date	Status	Action To Be Taken	Status Description
48	AR2006 25	2	Aycock, Mark Frankfort, David	8/31/2006	**In Process**	*Finding:* Significant weaknesses in internal controls over fixed assets in the data center. **ACTION 1**: Tag and revalue assets with added components. **ACTION 2**: Document & submit to I/A for review and approval.	