2015 Internal Audit Summary

Closed Audits: Recommendations

Audit Area	Risk Rating	Scope	Recommendations	Management's Response	Implemented	Implementation or Target Implementation
AIX/Windows Security*	Medium	Verify FTP Login is Restricted	Window Admin. Passwords: Change every 90 to 180 days to reduce the risk of unauthorized systems access	Alternate recommendation accepted ◊	Yes	2/27/2015
		Disabled Default Accounts				
		Registry Access Permissions	Privileged Access: Block login and remote-login to root account (set to values to "False") to increase security	Alternate recommendation accepted ¥	Yes	2/27/2015
		Domain/AD Model				
		Account Lockout Settings	AIX Password Settings: Align password configuration with industry best practices to reduce the risk of unauthorized access	Alternate recommendation accepted ±	Yes	3/1/2015
		Update Access				
		Review Groups				
		Comments:				
		◊ User-based Windows administrator accounts will be set to 180 days. Due to potential critical business interruptions, system/service based admin accounts will be manually changed at least every 24 months as part of the System Change Management (SCM) workflow.				
		¥ To avoid problems with Active Directory, "rlogin" will be kept disabled but value will be set to "True" to allow technicians to remote login. Changes made to all UNIX servers except AIX servers supporting the STaRS DB because the current Control-M system must run on "root". A product change has been requested.				
		± Non user-based systems (Oracle, Control-M, and TSM) passwords will be changed at least every 24 months to prevent potential business interruptions. SCM Tickets will be opened on/before 2/27/2015.				
Alternative Investments*	Medium	Opportunistic/Diversified: Due Diligence	Revise policies and procedures to include specific details on the execution of the monitoring process	Agree	Yes	6/30/2015
		Monitoring				
		Valuations				
Alternative Investments*	Medium	Private Equity: Due Diligence	Develop a formal process to ensure monitoring activities are properly performed and documented by individual analysts.	Agree	Yes	9/30/2015
		Monitoring				
		Valuations				
Database Security (Oracle)*	Low	Security and Password Configurations	Password parameters for key systems and applications be set to expire every 90-180 days.	Agree	Yes	5/28/2015
		Access to Database Listeners				
		Default Accounts and Passwords	Reduce the risk of attacks by changing NTS port from 1521.	Alternate Recommendation Accepted	No	6/30/2016
		Host-Based Authentication Methods				
		General Password Settings				
		Comment:				
		Internal Audit has accepted an alternate recommendation to, in the near term, increase protection through the use of application firewalls. As part of the larger, future project (Vitech upgrade, V10), ITS will work with Vitech to change the port.				
International Investing*	Low	External Manager Fees	Review the foreign tax reclaim process to reduce the risk of inaccurate or insufficient calculations and collection of receivable funds	Agree	Yes	12/12/2014
		Monitoring of External Managers				
		Foreign Tax Reclamations				
		Sub-Custodian Controls	Work with custodial bank to develop and deliver appropriate month-end reports	Agree	Yes	12/12/2014

Member Data Management*	Medium	Third-Party Access to Member Data Transmission of Member Data/Security Third-Party Operations/Control Contractual Agreements	Require routine sign-off of data owners to verify accuracy of tracking information related to the sharing and security of member data.	Agree	Yes	2/28/2015
Member Income Taxes	Low	Withholding Change Reconciliations Tax Interface Reconciliations Segregation of Duties	Review segregation of duties for shared access to STaRS processing screens	Agree	Yes	3/31/2015
Survivor Benefits	Low	Benefit Calculations Student Benefits Segregation of Duties	Until the new law is implemented, perform periodic, random sampling of student enrollment to verify compliance	Agree	Yes	9/30/2015

Closed Audits: No Recommendations

Audit Area	Risk Rating	Scope	Management's Response
Child Care	N/A	Compliance with State Licensing State Inspections Tuition Payments Enrollment	
Disability Benefits*	N/A	Reexamination Schedules Medical Invoice Payments Statement of Employment/Earnings Terminated Benefits - Notification Benefit Calculations	
Financial Reporting	N/A	Role-Based Security/Segregation Adjusting Journal Entries Disaster Recovery Audit Trail Integrity	
Fixed Assets	N/A	Tracking, Reporting and Monitoring Depreciation Disposition	
Health Care*	N/A	Records Retention/Management Issues Monitoring and Resolution Disbursement Reconciliations Segregation of Duties	

Liquidity Reserves	N/A	Compliance Income Purchases/Sales	
Member Withdrawals	N/A	Compliance Refund Estimates/Payments Non-Zero Accounts Segregation of Duties	
Personal Investment Disclosure	N/A	Compliance with Policies Accuracy/Completeness Monitoring	
Post-Retirement Benefits	N/A	Death Match Annuity Certain Expirations Overpayments/Collections Disbursement Compliance	
Service Retirement Benefits	N/A	Departmental Process Documentation Benefit Calculations Management of Overpayments Segregation of Duties	

Active Audits

Audit Area	Risk Rating	Scope	Target Completion
Accounts Payable	N/A	Vendor Approval Process Vendor Payment History Compliance with Policy Segregation of Duties	May-16
Alternative Investments*	N/A	Private Equity: Due Diligence Monitoring Valuations	April-16
Attendance Reporting	N/A	Accuracy Compliance with Policy	March-16
Building Maintenance	N/A	Purchases of Goods and Services Preventive Maintenance Associate Training Quality Assurance	April-16
Business Continuity Plan (BCP)	N/A	Compliance Monitoring & Testing	March-16

Board Expenses	N/A	Preapproval of Travel Accuracy of Reimbursements General Compliance with Rules/Policy	May-16
Domestic Equities*	N/A	Compliance with Investment Policy Monitoring of External Portfolio Managers Investment Management Fees Reporting/Accounting Research Costs Approved Brokers Custodian	May-16
Fixed Assets - Computer Equipment	N/A	Purchasing Accuracy of Inventory Records Disposition	June-16
Fixed Income Investments	N/A	Due Diligence Approved Brokers/Commissions Accuracy of Pricing Interest Income Monitoring of External Managers Compliance with Investment Policies	April-16
IT Security: B.Y.O.D. (Bring Your Own Device)	N/A	Compliance	January-16
OEC Reporting	N/A	Compliance	January-16
Postage	N/A	Compliance with Policies and Procedures Disbursements	December-15
Real Estate	N/A	Property Management Fees Site Inspections External Compliance Reviews Tenant Surveys Compliance with Investment Policy	June-16

Scheduled Audits

Benefit Payment Process	N/A	Accuracy of Monthly Forecast Reconciliations G/L Postings Segregation of Duties	March-16

Postponed Audits

IT Security: HIPAA		Awareness & Education Project Planning	N/A
		Comment: Reprioritized higher risk reviews resulting in the postponement of this audit.	

Other Audit Related Activity

Area	Risk Rating	Subject/Project	Description
I.T.S.	N/A	STaRS Upgrade	Consult with ITS and the user community on the security functionality and needs of the system.
Multi-departmental	N/A	DLP (Data Loss Prevention)	Participate on the DLP Committee to implement, monitor and evaluate the data loss prevention as it should function at STRS Ohio.
Multi-departmental	N/A	STRS Ohio Disaster Recovery	Participate in disaster recovery testing review. Strategize on business and human resource needs.

* Audits were listed as "Under Mgmt. Review", "In Progress", "Audit Initiated", or had not implemented recommendation(s) at the time of the last Annual Audit Summary presentation.

Risk Rating Level: (Refers to rating assigned to findings/recommendations)
High: Requires Immediate attention and remediation.
Medium (Med.): Requires near-term attention.
Low: Improvements possible but does not require attention in immediate or near-term.

Composition of Current Audit Committee:
Carol Correthers, Chair/Liaison - Active Member
Tim Myers, Vice Chair/Asst. Liaison - Active Member
James McGreevy, Retired Member
Craig Brooks, Appointee
Mark Hill, Appointee
Robert Stein, Non-Voting Observer