

2008 Audit Preparation

Meeting Outline

- Audit Purpose
- Auditor Information
- Audit Process
- Audit Schedule
- Audit Preparation
- Audit 2005 Follow-up
- Things I Know for Sure
- Questions

Audit Purpose

Office of Internal Auditing (OIA)

“Internal auditing is an independent appraisal activity authorized by the Board of Regents to examine, evaluate, and advise components of the University System of Georgia. The objectives of internal auditing are to assist members of the Board, the Chancellor, and institution management in the effective discharge of their responsibilities by furnishing them with analyses, appraisals, recommendations, counsel, and information concerning the activities reviewed and by promoting efficient operations and effective controls.”

Audit Purpose

- Annual Audit Plan
 - Designed to ensure coverage of institutions with high risk
 - Also designed to ensure OIA coverage at all USG institutions at least once every 3-4 years
 - Specifies institution and broad categories in which to audit
 - May also incorporate consulting engagements and other special projects

Audit Purpose

Audit Scope

- **Identity Management;** the management of user credentials and the means by which users might log onto to and use various systems or resources, e.g., the provisioning and de-provisioning of student, faculty, staff, and outside agencies identities
- **Access Control;** the mechanisms in place to permit or deny the use of a particular resource by a particular entity, e.g., technical or administrative controls to allow or deny access to file shares
- **Perimeter and Network Security;** the provisions made in an underlying computer network infrastructure to protect network-accessible resources from unauthorized access and the effectiveness of these measures.

Auditor Information

- Background Information:
 - IT Auditor for USG since March 2007
 - US Army – June 1987 – February 1992
 - Chaplain in USAF Reserves since 1999
 - Instructor at Chattahoochee Technical College from July 1997 – March 2007
 - Education: Working on MSIS at Kennesaw State University, MDIV from Regent University, BM from University of Missouri-Kansas City
 - Certifications: CISSP, INFOSEC, CSSP, CCNP, OCM



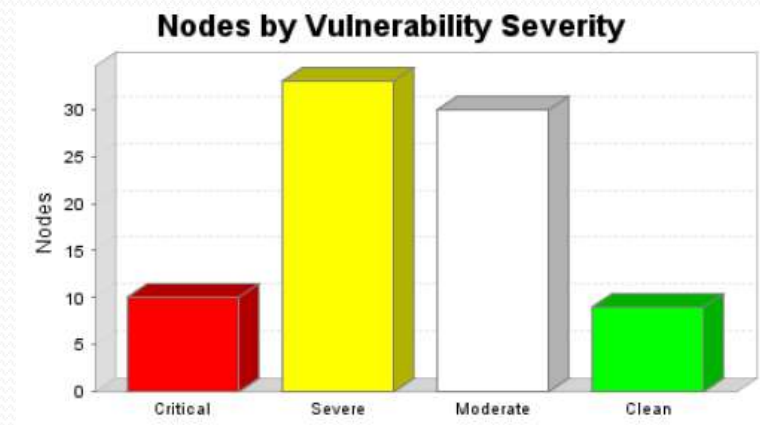
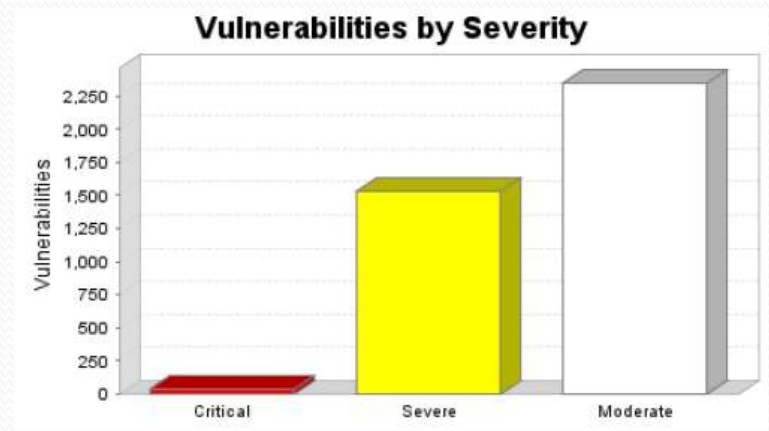
Audit Process

- Information Collection
- External Scan
- Internal Scan
- On-Campus Interviews
- Dialogue of exceptions and findings
- Exit Interview
- Preliminary Report
- UWG Response
- Final Report

Audit Process

External Scans

- Began Scans on 10/26/08
- Identified 46 systems from off-campus
- Only 1.02% (40/3913) of vulnerabilities were critical
- ITS has begun reviewing findings and addressing issues
- Many false positives
- Final update due 11/25/08



Audit Schedule

- Will Conduct 1-hour interviews with designated supervisors/employees
- Departments/Units selected based on IT Systems or Services used
- Entrance Meeting – November 10, 10am
- Daily Debriefing – Kathy Kral & Cathy Osborne
- Exit Meeting – November 25, 2pm

Audit Schedule

Areas to Visit

| | |
|--------------------------------|---------------------------------------------|
| Academic Affairs, VP | Health Services |
| Admissions | Human Resources |
| Auxiliary Services | Institutional Research & Planning |
| Bookstore | ITS |
| Budget Services & Asset Mgmt | Parking & Transportation Services |
| Bursar's Office | Registrar's Office |
| Business & Finance, VP | Sports Medicine |
| Continuing Education | Student Affairs & Enrollment Management, VP |
| Controller's Office | Townsend Center |
| Development & Alumni Relations | University Advancement |
| Financial Aid | |

Audit Schedule

Systems to Review

| | |
|---------------------------|---------------|
| Aceware/Aceweb | PeopleSoft |
| Banner | QuickScrip |
| Campus Loan Manager | Raisor's Edge |
| Catalog Submission System | Sportsware |
| Choice Ticketing System | Touchnet |
| ID Cards | Xtender |
| Nebraska Bookstore | Webchecks |
| Parking Ticket System | |

What Does He Want to Know?

IT Units

- Service Providers
- IT Policies
- Technical Implementations
- Operational Procedures
- Identity Management/Access Control (Technical)
- Network Security

What Does He Want to Know?

Non IT Units

- Business Function
- Operational Procedures
- Roles and Responsibilities
- Information Handling
- Identity Management and Access Control (Business)

What Can He Do?

He will be required to sign an authorization agreement

- Acknowledges confidentiality of information
- Agrees not to share or disseminate
- Must inform user and ITS of collection of information
- No data may be modified or deleted from any system
- Collected data must be destroyed once audit purpose is completed

What Can He Do?

System Access

- Computer Scans – He may or may not ask to scan your computer
- Collect Data – He may store information from a scan for reference
- Passwords – He does not have any rights to password information

Request Documentation

Request Follow-up Meeting/Discussion

The Interview

- One hour interview with supervisor
- One hour interview with employee
- Will be conducted at interviewees location
- Auditor Liaison will take auditor from location to location
- Supervisor will take auditor to employee (when meetings are adjacent)
- Supervisor will contact Liaison when auditor is with employee
- Contact Brenda Valcke immediately if there are any events that will affect your assigned interview time (x94002 or bvalcke@westga.edu)

The Interview

Handling the Interview

- Don't feel threatened
- Be Positive
- Answer the questions he asks
- Answer only what you know
- "I don't know" is OK with follow up

The Interview

Handling the Interview (continued)

- Remain calm despite his questions or responses
- Silence is OK
- This is not the time to vent

What If He Finds Something?

- He's going to find things
- There are levels to findings
 - Insignificant
 - Notable
 - Significant
 - Major
- He will notify us of his findings during the daily debriefing
- Contact me with questions or thoughts (ddriver@westag.edu or x94907)

Things You Need to Do

Review Operational Procedures with staff

Clean up personal items from computers

- Some pictures OK
- Incidental emails OK
- No financial information, excess music, other personal information

Don't leave your offices open

Enable screen-saver with password lock

Remove any password notes from desktop area

Things You Need to Do

Look around your area for physical issues

Talk to your Student Assistants about the audit

- No working on homework
- No surfing the web
- Be sure you have signed confidentiality statements for those who have access to such information

Have documentation available

- Policies, procedures, reports
- Contracts with 3rd party vendors (if necessary)

Audit 2005 Update

1. Governance Structure
2. IT Policies/Procedures
3. Network Security
4. Consolidate Services
5. Backup Tape Storage
6. Off-site Backup
7. Fire Suppression System
8. Fire Extinguishers
9. CS Server Room cooling
10. Employee Separation Notice
11. Pharmacy computer
12. Oracle DB permissions
13. Online PeopleSoft reports
14. Oracle DB configuration
15. HR Separation of Duties
16. Bookstore Credit Card information storage

Audit 2005 Update

- IT Policies and Procedures
 - Possible finding if current policy set is deemed inadequate
 - ITS Reorganization lends itself to better development of policies and procedures
 - IRP, DRRP, IT Security Plan, IT Strategic Plan are either in development or revision stages
 - Need to expand and integrate Business and IT policies and plans

Audit 2005 Update

- Notification System for Employee Separation
 - Developed an email form for separation notification in 2005
 - Does not accommodate transfers or role changes
 - Possible finding based on the questions provided by auditor
 - Demonstrates the need for correlation of business procedures with IT procedures

Audit Preparation

- We Are Who We Are
 - Early stages of IT reorganization
 - Have not officially adopted a defined IT Standard (looking at ITIL)
 - Have not matched business operations to IT Standards
 - Growing University with limited (shrinking) resources

Things I Know For Sure

- The Audit won't last forever
- There will be findings
- We won't agree with all findings
- We will grow from this experience
- We will be better from this experience
- I'm going to really enjoy Thanksgiving

Questions?