auditing IT

RESOURCES AVAILABLE

- INFORMATION SECURITY & ePRIVACY
  www.usg.edu/infosec
- USG SECURITY ADMIN LISTSERV
  USGSECURITYADML@listserv.uga.edu
- ARCHIVED WIMBA SESSION: PREPARING FOR AN IT AUDIT
  December 8, 2011
  www.usg.edu/gafirst-fin/training/archives
- ITS HELPDESK
  www.usg.edu/customer_services
  for business impact emergency issues:
  706.583.2001 or 1.888.875.3697

Why Worry about an IT Audit?

The role of information technology (IT) control and audit has become a critical mechanism for ensuring the integrity of information systems (IS). IT control and audit procedures also aid in preventing security breaches.

IT auditing is an integral part of the audit function because it supports the auditor's judgment on the quality of the information processed by computer systems.

The IT auditor's role has evolved to provide assurance that adequate and appropriate controls are in place. Of course, the responsibility for ensuring that adequate internal controls are in place rests with the management. The audit's primary role, except in areas of management advisory services, is to provide a statement of assurance as to whether adequate and reliable internal controls are in place and are operating in an efficient and effective manner.

Board of Regents of the University System of Georgia
Information Technology Services
2500 Daniells Bridge Rd.
Athens, GA 30606

Visit us on the web:
www.usg.edu/audit
www.usg.edu/gafirst-fin
www.usg.edu/customer_services

Contact ITS:
helpdesk@usg.edu
706.583.2001
1.888.875.3697 (toll free within Georgia)

User Management in PeopleSoft Financials

User Management in PeopleSoft Financials is a key component of protecting your organization's data and maintaining system integrity. It is vital that an organization limit privileged user access to a small number of personnel and hold those personnel accountable for maintaining their system users.

New User Access

Is the user authorized to be in the system? Are the appropriate forms or documentation in place that dictates the user's level of required access? Does that documentation contain the required level of authorization? The local security administrator should be careful to ensure that the level of access authorized is limited to only what that user specifically needs. Too much access could result in segregation of duties issues which is a BIG audit finding!

User Maintenance

This is probably the hardest level of user management to track. Each time a user changes positions or transfers departments, a through security review is required. This review should not be limited to user roles. User preferences, commitment control budget override authority, and approval access is a critical component of security access as well. This access works hand in hand with the users security access. New forms and authorizations are needed for every transfer or position change.

User Termination

It is critical that each institution have it's own business process for handling terminations. The human resources department should provide the finance department with a listing of terminations at least weekly, but it should be proactive when the situation allows. (See the section below for a discussion of tools to help assist with this.) Upon notification, the local security administrator should immediately lock the user's account and remove the base role. User preferences, budget override access, and approval access needs to be removed to ensure that transactions in the system do not continue to route to a terminated user. It is vital to an IT audit to keep up with your terminations!

Campus Security Tools and Processes

On April, 18, 2012, a Campus Security Guide was sent out from ITS that contained a checklist of items that the local campus security administrators should be looking for at a minimum. This guide also contains campus security tools, processes, and queries that will assist with identification of potential audit issues. The guide can be found on the Georgia*FIRST* Financials website.

The Campus Security Guide is meant to be used as a tool and a secondary method for identifying potential audit issues. **It is the responsibility of each individual campus to ensure that changes in personnel status result in immediate change in access to PeopleSoft Financials System as well as any other system of which the user is a part.**

Each campus must document and have a primary procedure in place for handling new hires, position transfers, and terminations.

BOR_SEC_TERMINATED_USERS Query

As local security administrators, it is imperative that the results of this query are closely monitored, reviewed, and validated. Once the campus has followed its primary procedure for terminations, the BOR_SEC_TERMINATED_USERS query can be used to validate that all terminations have been handled within the PeopleSoft Financials system. Users that appear on the query will need to be reviewed to ensure that they are truly terminated and are not a multi campus user.

SEGREGATE_DUTY_BOR Query

The Segregation of Duties query lists users with potential audit issues. However, it is not always the case that there is an issue. User preferences, in conjunction with certain security roles, will allow users to have too much access. It is vital that security as a whole is evaluated, and not just place the focus on security roles.

If a user does have a segregation of duties issue, then either (a) remove the offending roles or (b) each campus must create a proper compensating control and documentation must be kept proving the controls were kept, if the business area agrees to the increased risk.

What is an IT Audit?

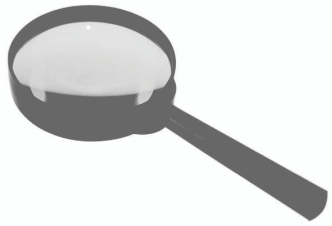
An IT audit is an examination of the checks and balances, or controls, within an information technology group.

- Collects and evaluates "evidence" of an organization's information systems, practices, and operations
- Determines if the information systems are:
  - ◊ safeguarding the information assets
  - ◊ maintaining data integrity
  - ◊ operating effectively and efficiently to achieve the organization's business goals or objectives

Auditors are interested in ensuring data integrity, availability, and confidentiality.

Auditors are looking for:

- General Application Controls
- Backup Procedures
- Monitored and documented job scheduling



There are nine ways to maintain General and Application controls:

1. Strong password settings
2. Limit privileged functions
3. Maintain segregation of duties
4. Ensure appropriate user access and authorization
5. Maintain general security settings
6. Control access
7. Change management
8. Maintain segregation of duties within change management
9. User acceptance testing