Internal Control Assessment training is scheduled for **February 24th at 2:00 p.m.** in the Human Resources training room. To sign-up, please email auditing@olemiss.edu.

Things to think about when preparing for an Internal Control Assessment

**INFORMATION SYSTEMS**

**Security Controls**

**Physical Controls**
- Physical controls help to protect against physical damage of the equipment (computer hardware, servers, etc.) from environmental exposure such as excessive dust, water, etc.
- Help to protect against theft of university assets (Computers in common areas and all laptops should be locked to a piece of furniture to avoid easy removal.)
- Access to servers with mission critical and/or confidential information should be monitored and limited to authorized personnel.

**Logical Access Controls** (Basically how does the department restrict access to data on machines and servers)
- Is access to university records protected (i.e. use of passwords) and are transaction and access logs kept/available? Internal Audit recommends to password protect screen savers.
**Tip! Do not write passwords down, nor display them visibly. Choose strong passwords, no dictionary words (Strong passwords are 6-8 characters long with upper and lower case letters, numbers and symbols). Never share passwords.**

» What user accounts are on desktops and laptops? Are they necessary?
» Are user accounts disabled/deleted on servers after employee termination?

**Virus Protection and Operating System (OS) Patches**

**Virus Protection**

» Is the latest virus definition installed on all machines?
» Is the software configured to automatically receive the latest updates?
» The department should perform weekly full system scans on all machines, and a log of the scans should be kept (Note: Most anti-virus software will do this automatically if scans are performed).
» Is anti-virus protection needed for servers? If yes, is it updated on a regular basis?
» Servers should be firewalled.

» Servers should be registered with the IT department. To register a Server, please log into portal via [http://my.olemiss.edu](http://my.olemiss.edu), then click “Tools and Resources” tab at the top to get to the Server Registry.

**OS Patches**

» Are all machines set up to automatically receive the latest OS patches?
**Backup and Recovery Procedures**

The department should have written policies and procedures in place to aid in timely restoration of data and systems in case of an adverse event. Departmental personnel should ask themselves the following questions:

- What happens if our computers/servers crash? Do we have backups?
- Do we have recovery procedures in place?
- What backup procedure is best for us? For example, back up to a server, external hard drive, etc?
- Who is responsible for which duties during recovery?
- What are our procedures during the down-time?

We strongly encourage all departments to send at least one departmental representative to an upcoming Internal Control Assessment training session. If you have any questions, please feel free to contact us at 915-7017 or auditing@olemiss.edu.