Information Item:
Overview of Information Technology Services' involvement in State Audits

Background Information:
Information Technology Services is involved not only in the annual financial audits, but may also be the subject of detailed Information Systems audits by the Office of the State Auditor. Because these can be very different kinds of audits, the attachment summarizes for the BOT Audit Committee the ITS role in each kind. Associate Vice Chancellor Laura Young will meet with the Committee to review this.

Attachments:
Overview of UNCG ITS involvement in State Audits

James Clotfelter
Vice Chancellor for Information Technology Services & Chief Information Officer (CIO)
Overview of UNCG ITS involvement in State Audits

Background
Two types of audits at UNCG require participation from Information Technology Services (ITS). Historically, the Office of the State Auditor has conducted periodic audits of enterprise information technology systems at each agency and University. The first audit category is known as Information Systems (IS) Audits. These audits occurred on a variable schedule, dependent on resources in the Office of the State Auditor (OSA), but were typically 3 to 5 years apart. Such IS audits have been broadly scoped, encompassing not only financial systems but also could include in scope desktop workstation and servers and databases not associated with University financial or student systems. The second audit category has been tightly coupled with the annual financial audit, and focused on general controls for access to financial systems.

IS Audit
The traditional IS audit at UNCG is focused on the ITS division of the University. It begins with an entrance conference involving the Vice Chancellor for Information Technology, key ITS staff members, the university internal auditors, and the state audit staff. The engagement can take several weeks (or even months) to complete. A UNCG ITS audit liaison is identified, usually the Associate Vice Chancellor for Administrative Systems. ITS receives questionnaires and lists of requested materials from the State audit staff. Typically, OSA does not request a recitation of any past events or breaches but instead focuses on controls and preventative measures. Requested materials usually include but are not limited to:

- a variety of system logs for access control to systems, applications and databases
- logged information for physical access control to machine rooms and wiring closets
- the Disaster Recovery Plan, along with evidence of annual testing
- information about the versions of applications and operating systems in use
- system operation policy and practices
- application system development policies, practices and methodologies
- application system maintenance policies, practices and methodologies
- network diagrams and network security information
- staff training information
- environmental, health & safety items such as emergency exit signs, fire suppression systems and security monitoring cameras
- University strategic planning information and information on the alignment of Information Systems planning
- information on technology systems attached to the network that are not managed by central ITS

ITS staff retrieve and package the data and securely transmit it to the Office of the State Auditor. This entire process can take hundreds or even thousands of man-hours of work for University staff, with the
bulk of this effort in ITS (there is some work from Business Affairs, but this is targeted around application general controls only). Each cycle of the IS audit usually brings additional items into scope. Due to the comprehensive nature of this engagement and its continuing growth in scope and coverage, it is essentially impossible to receive a completely clean audit with no findings.¹ We strive to ensure we only have minor findings, as the major findings are usually associated with core competencies where we understand expectations and have appropriate competencies and controls. UNCG was last contacted by the Office of the State Auditor for an IS audit in 2010, but the OSA decided to cancel the audit due to their own resource limitations just two weeks before they were scheduled for the entrance conference. UNCG had already invested much of the time it expected to expend on the 2010 audit by the time we were notified of its cancellation. ITS staff subsequently has had numerous conversations with OSA staff and they indicate that the OSA is changing its paradigm on audits and will not be performing IS audits, or doing them very infrequently. However, we have seen no written statements that confirm or deny this observation. UNCG’s last full IS audit was in 2004.

**IS Component of Annual Financial Audit**

For years, there has been some ITS involvement in the annual financial audit. Historically, this has not required extensive effort from ITS, as ITS has been only in a supporting role, providing a summary of information about general controls. The entrance conference of the financial audit is with OSA, the Vice Chancellor of Business Affairs and, only optionally, ITS representatives. While the breadth of coverage has typically included questions about operating systems, application controls, application development, application maintenance, operations, physical access, and more (many of the same areas in the IS audit), responses have been limited to one or two paragraphs for each area, without the requirement for large amounts of supporting evidence. Starting in 2012, consistent with information relayed from OSA staff to UNCG ITS staff, the scope of the IS component of the annual financial audit grew to include requests for more detailed responses to questions and included requests for many of the types of evidentiary information (i.e. system log extracts) that were formerly only requested in the IS Audit. In 2013, OSA staff asked UNCG ITS staff to review the 2012 questionnaires and document any changes in areas highlighted by the OSA staff. The 2012 questionnaires required substantially more effort than any preceding financial audit (but still only a fraction of the total effort of the legacy IS audit), while the process followed in 2013 was much more streamlined, focusing only on changes. We are optimistic that this model will be followed in the future.

**Audit futures**

We have discussed the changes in the audit process with senior auditors from OSA. They indicate in personal conversation that the overarching trend is to try to work smart, looking at changes in systems rather than reviewing everything, every time, and focusing on areas that have been shown empirically to be problematic. Additional focus will be placed on emerging issues such as use of server virtualization. The new approach from OSA is sound and is more efficient in the use of resources from both the OSA and the audited institution. We will continue to monitor this very important area.

¹ For example, a 2010 IS Audit at one of The UNC system's large campuses led to seven major, public findings, plus an additional five confidential findings.