Higher Education Compliance Challenges

INSIDE:
- Building a Compliance Program
- Electronic Workpapers
- All the Cash, Much of the Risk
- Medical Records
- Audit and Compliance
- Computer Assisted Audit Techniques
FEATURES

ACUA LIFE
4 Meet Your ACUA Board Members — Phil Hurd and Tina Maier
By Brenda K. Mowers

5 Inside ACUA-L
Compiled by Brenda Mowers

INTERNAL AUDIT ORGANIZATION
7 Building a Compliance Program in Higher Education Institutions Without Compliance Officers
By Susan Keller

INTERNAL AUDIT PRACTICES
11 Electronic Workpapers (On the Cheap)
By Mel Hudson-Nowak

HIGHER EDUCATION
14 All the Cash, Much of the Risk, But Too Few of the Curbs
By Mariamme M. Jennings

17 Medical Records: Signed, Sealed and Secure
By Kay Hardgrave

21 Audit and Compliance: Understanding the Difference
By Andrea Claire

COLUMNS
23 Addressing Common Barriers to Using CAATs
By Donald E. Sparks

DEPARTMENTS
1 From the Editor
2 From the President
3 From the Executive Director

ACUA members are invited to submit letters and original articles to the editor. Go to www.acua.org and click on the FAQ and Publication for further guidelines. Please send your copy electronically to the editor or ACUA in Word 95 (or higher) or text file format. The editor reserves the right to reject, abridge or modify any advertising, editorial or other material.

Editor
John M. Fuchko, III, MBA, CIA, CCEP
Board of Regents/
University System of Georgia
john.fuchko@usg.edu
(404) 656-9439

Contributing Editors
ACUA Life: Vacant
Internal Audit Organization:
Claire Sams Milligan,
Alabama Department of
Postsecondary Education
Internal Audit Practices:
Mel Hudson-Nowak,
Bowling Green State University
Higher Education:
Michael J. Foxman,
University System of Georgia
Columns:
Sterling Roth, Georgia State University

Copy Editors
ACUA Life:
Brenda Mowers,
Montana State University – Bozeman
Donna Stapleton,
Technical College System of Georgia
Internal Audit Organization:
David Dixon, Governors State University
Internal Audit Practices:
Amy Hughes,
Michigan Technological University
Higher Education:
Mary Ann MacKenzie,
Auburn University
Columns:
Beverly Hawkins-Llewellyn,
The University of Montana

ACUA Management
Stephanie Newman, Executive Director

College & University Auditor is the official publication of the Association of College & University Auditors. It is published three times a year as a benefit of membership. Articles in College & University Auditor represent the opinions of the authors and do not necessarily represent the opinions of governance, members or the staff of the Association of College & University Auditors. Acceptance of advertising does not imply endorsement by ACUA. ©2009 Association of College & University Auditors.

Send address changes to:
ACUA
PO Box 14306
Lenexa, KS 66285-4306
ACUA-info@goamp.com
Professionals in the field of higher education auditing and compliance need not look far when considering the potential risks faced by their institutions. Our spring 2009 CandU Auditor theme is “Higher Education Compliance Challenges.” This edition is our attempt to provide readers with some clear perspectives on how a compliance program might reduce both the likelihood and the impact of some of the potential risks that internal auditors are called to assess.

However, a “clear perspective” is not always easy to find. Genuine differences exist on the role of internal auditing in the compliance arena. Some professionals see a compliance program as entirely distinct from internal audit. Other professionals believe that internal audit should help to start the compliance program while preparing the program for eventual independence from internal audit. Still other professionals might suggest that a compliance program has a permanent place in the internal audit department, albeit with some distinction between the internal audit function and the compliance function. We have attempted to include authors who represent these various perspectives and we will leave it to the reader to sort through the best solution for his or her institution.

BRIEF OVERVIEW AND FUTURE ISSUES

This edition includes an article by our very own Mel Hudson-Nowak on how an institution might implement electronic working papers using a standard Microsoft Office product. Mel also produced two articles for our winter 2009 issue. We certainly appreciate her commitment to sound articles that add value to this publication. Susan Keller provides some excellent insight on how an institution without a compliance officer might go about establishing a compliance program while Andrea Claire helps to clarify the difference between an internal audit function and a compliance function. Kay Hardgrave provides some practical advice on auditing medical records. Donald Sparks serves as a guest columnist with his column on using computer assisted audit techniques. Finally, Marianne Jennings makes an excellent case for the importance of ethics in higher education.

Our Summer 2008 edition will focus on “Globalization & International Programs: Risk & Opportunity.” Several interesting articles are already lined up for this issue to include an article on the difference between GAAP and IFRS and another article on understanding SAS 70 reports. We also expect to see an article on study abroad programs, best practices in managing internal audit and a column on information age fraud schemes. We will be establishing our themes for the next year’s issues prior to the ACUA Annual Conference. Reader suggestions and feedback are certainly welcome!

On the lighter side, our ACUA Life section includes our President’s perspective on audit and compliance. Also, we have the opportunity to hear from our new Executive Director, Stephanie Newman. Readers are also provided a short introduction to ACUA Board Member Phil Hurd and ACUA Board Secretary/Treasurer Tina Maier. Finally, Brenda Mowers has once again done an excellent job of highlighting and summarizing some recent ACUA-L postings.

HOUSEKEEPING

I already noted that the editorial staff would certainly appreciate any feedback or ideas that our readers might have as it pertains to future themes and articles. Please feel free to send me your thoughts at john.fuchko@usg.edu or you can call me at 404-656-9439. Also, please note that we have several vacancies on our volunteer editorial staff. Mel Hudson-Nowak is leaving her role as Internal Audit Practices Section Editor. Mel will continue to write for the journal and I am pleased to announce that Amy Hughes will step up from her role as Internal Audit Practices Copy Editor into the role of Section Editor. However, we still have vacancies in the ACUA Life Section Editor position and in the Internal Audit Practices Copy Editor position. Interested individuals should contact me.
ACUA members have strong ties with compliance functions. Many of our members are responsible for the compliance functions at their institutions and our association has been very supportive of compliance activities. There is a compliance track at our annual conference and our midyear conference usually includes many compliance related subjects. Additionally, ACUA has been a sponsor over the last several years of the Conference for Effective Compliance Systems in Higher Education hosted by the Society of Corporate Compliance and Ethics.

Other than ACUA President, I am one of those ACUA members with dual responsibility. My job is executive director for Audit, Compliance & Risk Services at The University of Texas at San Antonio. There are two separate offices that report to me. The Office of Auditing & Consulting Services functions as does any other audit activity. I view that office as a detective control providing assurance that high risks are being mitigated to an acceptable level and that the institution is operating efficiently and effectively.

The Office of Institutional Compliance & Risk Services, on the other hand, functions as a preventive control. Its primary purpose is to provide tools to the campus community that enable the campus to know and understand compliance high risks and then to “do the right thing” and reduce negative outcomes. The close working relationship necessitates significant coordination and collaboration between the two functions.

Keeping in mind that my institution is an academic institution without a medical school, here are some of the primary responsibilities of the Compliance function:

- **Risk Identification** – assisting management with identification and prioritization of compliance risks
- **Risk Ownership** – identification of institutional risk owners
- **Risk Management** – assisting management with developing plans to manage high risks
- **Awareness** – promoting awareness and providing general compliance training
- **Monitoring & Assurance Activities** – providing a confidential reporting mechanism (hotline) and conducting inspections to ensure high risks are being adequately mitigated

**RISK IDENTIFICATION**

Annually, we perform a university-wide risk assessment by providing the President, Vice-Presidents and senior administrators with a comprehensive list of higher education areas. They score each risk for the impact it may have and probability of the risk occurring. This list is very similar to the list in the ACUA Risk Dictionary. We then assign a ranking to each item based upon the score given and determine which items are of highest risk to the institution. The final list is usually around ten to twelve areas and is approved by the Executive Compliance Committee. It is important to note that we will “drill down” from the executive level risks to the operational level in order to ensure that all risks identified have been addressed from the “C suite” to the cubicles.

**RISK OWNERSHIP**

After the high risk list has been approved by the Executive Compliance Committee, each high risk area is assigned to an Institutional Risk Owner (IRO). Although there may be crossover among vice presidents, we assign one individual as IRO. This is usually a vice president for whom the authority to take action is most appropriate.

**RISK MANAGEMENT**

Each department or area that has some responsibility for a high risk area is required to develop a management plan to mitigate the risk to an acceptable level. The Compliance Office will offer assistance in developing those plans, but the ownership of those plans remains with the responsible area. Management plans address the seven components of the Federal Sentencing Guidelines to include: adequate procedures, training, reporting, monitoring and responsible parties.

**AWARENESS**

The Compliance Office works with subject matter experts to deliver annual general compliance training for all employees. Much of this training is required to be completed by everyone on campus. This training includes:

- Ethics
- Fraud
- Sexual harassment
- Information security
- Campus safety
As I sit down to write this article, the transition to Applied Measurement Professionals (AMP) as ACUA’s management firm is well under way. Just like moving to a new home, there have been a few bumps along the way, a few items temporarily misplaced, and lots of boxes to unpack. Setting up a new home allows for reflection on past accomplishments as well as consideration of new possibilities. There are new friends and new challenges to meet but in the end there is the start of an exciting new adventure in a new place.

ACUA’s new staff members are:
- Stephanie Newman, Executive Director
- Megan Eastland, Association Manager/Meeting Planner (Midyear)
- Melissa Whitaker, Meeting Manager (Annual Meeting)
- Jeanetta (Jenny) Smiley, Administrative Assistant

These staff members are also supported by other AMP employees in our data administration, accounting and publishing divisions.

We have already had the opportunity to meet many of you over the phone and some of us have been able to meet you in person. We look forward to serving you and getting to know all of you better. Thank you for making us feel welcomed as part of the ACUA family.

Over the past few weeks, we have been setting up the basic infrastructure needed for the Association to run properly; everything from setting up a new phone number to customizing our database for ACUA’s membership data. Our goal is to make the transition as seamless as possible for ACUA members. We have appreciated members’ patience as we work out the kinks.

ACUA’s staff has also been working closely with the Board of Directors to evaluate every aspect of the Association and how it serves its members. Instead of cutbacks to benefits, however, we have been discovering ways in which we can reduce expenses by streamlining certain areas. It is our hope that we can use this savings to improve member benefits as well as to develop new products and services in the near future to better serve your needs.

Two of the most important ways in which ACUA serves its membership are through the midyear and annual conferences. Both conferences represent an excellent value for obtaining CPE in comparison to similar events. If you have not done so already, be sure to register for the Midyear Conference scheduled for April 26 – 29 in Austin, Texas. We were able to maintain 2008 rates for this year’s conference and in addition will be offering two courses (IT Auditing & Controls by the MIS Institute and IDEA version eight training by our Strategic Partner, Audimation) at a deeply discounted rate compared to what members would pay to attend these sessions elsewhere. Registration is available through the Events and Seminars section of the ACUA website at www.acua.org.

If you can not make it to Midyear, we hope that you will plan to attend the Annual Conference, September 13-17, 2009 in Minneapolis, Minnesota. The program is taking shape and is one that you won’t want to miss.

The staff is excited to be able to participate in this chapter of ACUA’s history. We look forward to the great adventures we will have together as we work to build ACUA’s future.

We look forward to meeting all of you in Austin and Minneapolis!
Phil Hurd

Phil is no stranger to ACUA’s Board; he has previously served in various capacities for nine years. In addition, he was ACUA’s Director of Distance Learning for two years and was recognized with the ACUA Excellence in Service Award in 2007.

Phil is the Chief Audit Executive and Director of Internal Auditing at the Georgia Institute of Technology. He holds professional certifications as a Certified Information System Security Professional (CISSP), Certified Information Systems Auditor (CISA), and Certified Business Manager (CBM). He has a Masters Degree in Information Systems from Western International University.

Phil joined Georgia Tech in 1999 as an IS auditor and was promoted to Director of Internal Auditing in 2007. Before joining Georgia Tech, he served in the U.S. Army Military Intelligence Corps for ten years. Phil has a wife, Daphne, and a three-year-old son, D’Artagnan Phillippe. They have four mixed-breed dogs, Sasha, Sam, Snuggy and Zoe. CandU Audit readers might be surprised to find that Phil met his wife online!

Phil senses an eminent change within the profession. One of his goals as a Board member is to influence that change.

TINA MAIER

Tina holds a CPA from Florida and has spent most of her professional career in that state. Tina is the Associate Director for University Audit at the University of Central Florida (UCF). She began working in University Audit at UCF as a senior auditor in 1990. Previously, Tina worked for the Office of the Auditor General from 1986 thru 1989. Tina plans to stay at UCF until retirement.

“I Love my job and I love UCF!” was one of the first things Tina communicated about her position at UCF.

Tina has been married to Earl for 27 years and they have three boys – the oldest boy is now attending UCF. Tina loves to go fishing with her husband at their favorite spot – Turtle Mound in New Smyrna, Florida – but only because Earl baits the hook and then un-hooks the fish they catch – she never has to touch a fish!

Tina believes that ACUA members would be surprised to know that, “While I love to mingle and I’m not shy, I’m absolutely petrified of public speaking!”

As Secretary/Treasurer, her top goal is to increase transparency of the ACUA financials. She would like every ACUA member to be aware of the expenditures needed to manage ACUA and feel comfortable asking about those costs. She also would like to see ACUA increase revenues. For many years, a deficit was budgeted and there has been minimal growth in investments. With the downturn in the economy, investments have dropped significantly. Also as auditors, she thinks it is very important to have adequate internal controls over our business process. She believes that AMP is getting ACUA closer to this goal with almost 100% compliance.

For Tina, the best way to get the most of your ACUA membership is to attend the annual conference. She proudly stated that, “You can’t get more relevant training and CPE anywhere else. I really like moving from one session to another and gaining knowledge on numerous topics. I also love the special events and like visiting new locations, let alone all the networking.”

She believes that volunteering is the second best boost for ACUA members. Volunteers get to work on a project outside of regular office duties which both spices up the work routine and also adds a nice touch to the resume … all while supporting ACUA.
One of the best benefits of ACUA membership is participation on ACUA-L. The listserv provides an opportunity for members to discuss internal audit operations with other members and is a means of disseminating information related to audit work. These are some of the topics discussed on ACUA-L in recent months. Subscribe today—help is only an email away!

AUDITOR INDEPENDENCE

As described by Don Holdegraver, one of the most usual postings was a question about auditor independence and objectivity. The inquiry was whether independence is impaired if the audit director is “required to conduct visits to classrooms to inform students of the last day to pay fees, add and drop courses and of scholarship funds available as part of the activities of the Enrollment Management/Academic Affairs units.”

Many respondents stated that being required to conduct classroom visits was an operational duty and that auditors should not be involved since this was strictly a management activity. Some respondents were also concerned that management did not appear to understand the role of internal auditing or that management’s view of audit might create a negative image within the institution. Phill Armanas, at the University of South Australia, weighed in with a different point of view. He wrote that when IA staff takes on occasional operational roles it could serve as an indication of IA’s commitment to management and gives auditors a better understanding of operational issues, as well as the ability to return to IA with a fresh perspective. Audit staff that takes on operational roles from time to time should not perform future audits in that area.

NCAA AUDITS

Auditor independence was also the focus of a question regarding the NCAA Agreed-Upon Procedures (AUP). Little did Susan Pimentel at Southern Illinois University know that her question would lead the NCAA to consider clarification to the procedures!

The question was that while the NCAA appears to allow system internal auditors to conduct the audit work, such work must be in accordance with the AICPA attestation standards (per required wording at the end of the AUP guidelines). Those standards prohibit internal auditors from performing the audit work, as generally internal auditors perform audit work in accordance with IIA standards. She wondered if anyone had insight into whether the report wording could be changed or left out, and if internal auditors truly should not perform the review unless they switch to AICPA attestation standards.

A lively discussion followed and eventually Jean Stewart of the University of Colorado asked the questions of Joyce Collins, Director of Accounting for NCAA Administrative Services. Joyce indicated that the NCAA would consider clarification the next time the NCAA revises the AUP. She also asked for suggestions on designations or certifications appropriate for performing the work.

MANAGING ANONYMOUS HOTLINES

Cutting costs are near the top of everyone’s list these days. Cindy Copes, from Saint Leo University, asked about the frequency of ethics hotline activity in small, private universities using a third-party vendor. Of those that responded, most had very few reports since implementing a hotline. One of the larger schools to weigh in reported “some very fruitful investigations” resulting from about 28 reports received over four years.

Pat Reed from the University of California System wrote that irrespective of institution size or governance (public vs. private), publicity is important to helping employees understand the importance of reporting suspect activities and that anonymity will be respected for those who do report wrongdoing. He also said that if you are not getting very many reports over the hotline, it might mean that your school’s environment is such that people feel comfortable coming forward without the added protection of anonymous reporting.

SAVING MONEY

Dominic Daher from the University of San Francisco posted an item asking for ideas on ways to generate additional revenues during these difficult economic times. He was looking for audits that have resulted in substantial cost savings or other forms of revenue generation.

- Pat Reed suggested audits of vendor contracts, especially where they are subject to A-21 cost allowability standards.
- Randy Ross from Winston-Salem State University proposed looking at gas cards usage by facilities employees. Some things to watch for are multiple purchases on the same day, purchases made out of the immediate area and/or purchases made before or after regular business hours.
- Maureen Cassidy of Loyola Marymount University added looking into controls over gas pumps located on campus. She also suggested checking overtime—and overtime monitoring.
- Fred Chavez at the University of San Diego recommended digging into the MPG that various university vehicles are getting. The concern is that when employees are not paying for gas themselves, there is no incentive to conserve gas. In addition, given the addition of sustainability to many institutional missions, gasoline usage also has a non-financial aspect to it.
- Rick Gfeller at the Arizona Board of Regents proposed performing construction audits for those campuses with construction activity.
- Joe Pickard with Pepperdine University advised that internal audit departments could add value by performing in a consulting capacity rather than performing a more traditional audit.
Conflict of Interest?  
**Debatable.**

Students Suffering the Consequences?  
**Not Debatable.**

Ensure conflicts of interest do not overshadow your institution’s focus on quality education. Global Compliance can provide you with a comprehensive ethics and compliance program to preserve the integrity of your institution. So, look to the ethics and compliance leader that already serves major colleges and universities across the country in addition to one-half of America’s Fortune 100 and one-third of America’s Fortune 1000.

- Code of Conduct
- Online Training
- Employee Communication Campaigns
- Hotline and Web Reporting
- Case Management
- Ethics/Compliance Program Evaluations

© 2009 Global Compliance. All Rights Reserved.
Building a Compliance Program in Higher Education Institutions Without Compliance Officers

By Susan Keller

It is commonly known that compliance requirements in higher education do not easily fall under one functional area. Rather, because higher education compliance requirements originate from so many different sources, they cut across many different functional areas, such as compliance for research and federally sponsored programs, NCAA athletics, environmental and safety compliance, accounting and financial reporting (IRS, GAAP and GASB); and regulations that were not initially intended for higher education, including the Gramm-Leach-Bliley Act and Red Flags Rules. Each compliance area has its own set of complex and ever-changing requirements and no one person can be expected to stay abreast of the latest developments. Regardless of the complexity involved in managing compliance, a breach in any of these areas can have serious consequences, including fines, penalties and reputation damage.

Colleges and universities have been struggling to find the most cost-effective and comprehensive means to tackle diverse sets of compliance requirements at a time when Boards of Directors, management and stakeholders are demanding transparency and accountability and pointedly asking what is being done about compliance. A number of large institutions have established a compliance function consisting of a compliance officer and staff. Others have established a compliance officer position; this officer leads a committee specifically convened to address compliance issues across the institution. Since budgets are tight, it is unclear whether creating this position in a smaller institution is prudent or practical. Nonetheless, adhering to compliance is critical to university governance practices.

Surprisingly, adhering to all required compliance mandates does not have to be a daunting task. Over the course of several years, a compliance program can actually be cost-effectively implemented in a five-step process driven by the internal audit (IA) function.

EMERGING TRENDS
The IA profession has been reshaped in recent years by emerging trends. Sarbanes-Oxley has elevated the importance of the IA function not only to Boards of Directors, but also to the entire business community at large, by emphasizing that IA brings to organizations “… a systematic approach to evaluate and improve the effectiveness of risk management, control, and governance processes” as stated in the International Professional Practices Framework published by the Institute of Internal Auditors. The Statement on Auditing Standards (SAS) No. 112 in the nonprofit sector also pushes for greater transparency, accountability and documentation of controls and compliance.

Since the governance structure in higher education is often decentralized, with no central person or program overseeing compliance, it can be difficult to know who exactly is responsible for ensuring compliance for all the disparate areas throughout the university. In addition, some functional areas within an institution may not embrace the perspective of the entire institution and thus, may not fully understand the importance of communicating with other operational areas to effectively cover compliance requirements that cross functional boundaries.

This is an excellent rationale for the IA function to drive the establishment of an institutional compliance program. IA is the one group chartered with a university-wide view of risk and control, and is positioned to cull, correlate and share information across the institution. IA is proficient at interviewing leaders so as to understand and document difficult issues, and it is IA’s responsibility and obligation to improve the university’s control environment. Thus, it would naturally follow that an obligation to improve the control environment includes helping the institution implement a formal program of compliance.

PROACTIVE UNIVERSITIES
More universities are doing just that – conducting formal, university-wide risk assessments and adopting some version of a structured risk management program that includes a compliance component. Many of these efforts are being led by the universities’ IA teams.

At Duke University, executive director of IA, Mike Somich, chairs the operating committee of the Institutional Ethics and Compliance Program..
which is composed of 12 individuals on campus with the greatest compliance responsibility. Mike Somich also coordinates the institution’s School of Medicine and Health System compliance officers. He developed a structure for institutional compliance to ensure the comprehensive assessment of risk and monitoring at appropriate levels.

Gail McDermott is the chief audit executive at Harvard University; she oversees the Risk Management and Audit Services (RMAS) function. To promote ethics and accountability across the university, RMAS developed a training program called “Ethics, Accountability and Internal Controls,” targeted to the Harvard financial community. This training has been delivered in the financial administration department, in three of the university’s schools with dedicated sessions and through the Center for Workforce Development. More than 2,000 financial and administrative employees have been trained in ethics, controls and the importance of compliance.

The University of Pennsylvania is another proactive, compliance-minded institution. There, Mary Lee Brown leads the Office of Audit, Compliance and Privacy (OACP). Ms. Brown and her team’s primary objective are to take a risk-based approach to the audit function. They spearhead education about risk and compliance across the campus and in various forums. They also have defined five types of business risk that are prevalent in both higher education institutions and corporations alike:

- **Strategic** – the overall direction of the organization
- **Financial** – the safeguarding of assets
- **Operational** – the heart of day-to-day operations and processes
- **Regulatory** – as local and federal laws and regulations become more complex
- **Reputation** – which affects both image and brand

Ms. Brown and the OACP team bring professionals in the university together to discuss these risks and consider them not just within their own realm, but also in the context of the institution as a whole. The OACP team also provides the tools necessary to examine, assess and monitor the risks.

As these examples indicate, IA functions at major institutions are deeply involved in leading and participating in compliance initiatives.

**BUILDING A COMPLIANCE PROGRAM: A FIVE-STEP APPROACH**

A compliance program is a formal, structured approach to documenting, inventorying and ultimately managing the university’s compliance efforts. Formalizing a compliance program will not only help ensure there are no compliance gaps, but will also provide assurance to outside parties and regulators that the university is concerned about compliance and actively engaged in managing adherence. Establishing a program can often be the catalyst for bringing the views of the board and executive leadership together with respect to compliance management and ownership. To be effective, a formal compliance program should be well-documented, easy to update and accessible for reference to everyone at the institution. Once formalized and documented, the program also can be used as part of a training vehicle for new faculty and staff.

A formal compliance program can be developed in a five-step approach. It is important to note that this is a continuous improvement process. Full implementation does not need to occur all at once; it can span several years. The compliance program should describe the plan and expected timeline to accomplish full implementation.

The five steps in the process to establish a compliance program are as follows:

1. **Build the foundation** – The first step involves outlining and documenting the program itself; in other words, why it is being established and what it intends to cover. This formal document must be clearly written and posted formally in a format that is easy for stakeholders to access and read. It should include:
   - The institution’s philosophy on compliance and what it expects to achieve from its compliance program
   - A description of the governance group (such as the board of directors or a subcommittee) that is ultimately responsible for the program
   - A description of the process used to build the program, such as the five-step process described in this article
   - A list of individuals who are responsible for the various steps in building the program
   - A realistic timeline for executing the program (this may span several years).

Once the outline of the program is written, it should be approved by a governing committee to ensure buy-in and demonstrate endorsement from university leadership.

2. **Identify the initial compliance inventory** – The second step is to identify and understand the functional areas where compliance is required, such as:
   - Sponsored Programs Regulatory
   - NCAA Regulatory Requirements
   - Tax Requirements
   - Financial Regulations
   - Employment Regulations
   - Facilities Regulations
   - Public Health and Safety Regulations
• Academic Regulations  
• Student-Related Regulations  
• Other Regulations: GLBA, HIPPA, USA PATRIOT Act, Exports, Lobbying, Restrictive Gifts, INS, Federal Sentencing Guidelines

Since many institutions have been compiling their own compliance inventories recently, a university would do well to start by benchmarking with other institutions to understand how peers have articulated and organized their compliance inventories. There are also resources and books available to help. One excellent resource is “Regulation and Compliance: A Compendium of Regulations and Certifications Applicable to Sponsored Programs” by Jane A. Youngers and published by NCURA, which clearly outlines and describes all compliance regulations for institutions accepting any federal research money.

This initial inventory can be augmented and personalized by engaging in a group discussion with key leadership from each of the university’s functional areas to more fully describe the project, increase awareness of the extent of compliance, and refine or restructure the format of the initial inventory of compliance to suit institutional needs. It may be helpful to use a spreadsheet similar to the following chart (or a database) to begin to capture this inventory and the supplemental information discussed in the next steps.

### Compliance Areas

- The Awards and Sponsored Programs Function
- OMB Circular A-21 Revised - Principles for Determining Costs Applicable to Grants, Contracts, and Other Agreements with Educational Institutions
- Title VI of the Civil Rights Act of 1964 - 42 USC 2000d et seq.

### Business Objectives

- OMB A-21 establishes principles for determining costs applicable to grants, contracts, and other agreements with educational institutions. The principles deal with the subject of cost determination so that the federal government bears its fair share of total cost.

<table>
<thead>
<tr>
<th>Compliance Areas</th>
<th>Business Objectives</th>
<th>Risks of Not Meeting Objectives</th>
<th>Inherent Risk Rating L/M/H</th>
<th>Elements of Managing this Risk</th>
<th>Responsible Official/Department</th>
<th>Monitoring Techniques</th>
<th>Residual Risk Rating L/M/H</th>
<th>Gaps</th>
<th>Relevant Links</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>OMB Circular A-21 Revised - Principles for Determining Costs Applicable to Grants, Contracts, and Other Agreements with Educational Institutions</td>
<td>No awards will be made to any institution without an Assurance of Compliance (which states it will take measures to meet all objectives of the statute) on file. This act extends comprehensive civil rights protections to individuals on the basis of race.</td>
<td>Sanctions for noncompliance: no awards made to an institution without an Assurance Certificate on file. Also violation of the assurance may result in loss of all federal funding.</td>
<td>H</td>
<td>Ongoing training and education for OSPR and Financial Accounting staff.</td>
<td>Mutual Responsibility; Office of Sponsored Research, Business Centers &amp; Central Offices (Purchasing, Travel and Controller’s Office).</td>
<td></td>
<td></td>
<td><a href="http://www.usdoj.gov/crt/corw.usdoj.gov/omb/circulars/aa.htm">http://www.usdoj.gov/crt/corw.usdoj.gov/omb/circulars/aa.htm</a></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Title VI of the Civil Rights Act of 1964 - 42 USC 2000d et seq.</td>
<td></td>
<td></td>
<td>H</td>
<td>Assurance on file and policies in place. See HR website, compliance &amp; reporting section and Board Policy XX.</td>
<td>Director of HR; AA plan is on-line.</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

In addition, an initial “inherent risk assessment” (the level of risk without consideration of existing or planned controls) should be made for each compliance area at this point.

3. Identify and document the compliance requirements – Next, prepare a work plan and timeline for capturing more detailed information related to compliance requirements for all functional areas of the institution. It is easiest to begin by diving deeply into one functional area to make sure the universe of compliance requirements is relatively complete and to identify the person or group responsible for understanding the regulations and compliance requirements.

Become familiar with key people in that function and conduct interviews to foster a mutual understanding of the applicable regulations, the risks and potential consequences of noncompliance and how compliance adherence is being administered. All of this information should be captured in a compliance spreadsheet, as the previous example indicates. The process used to conduct the first “deep dive” (such as interviews or facilitated discussions) can serve as the prototype to use for other functional areas later in the work plan.

4. Identify controls, policies and monitoring – Once the universe of regulation and compliance and the party responsible in a given functional area is known and documented, it is time to document the institution’s controls, policies, procedures and monitoring activities for that compliance area. Recognize that this is where gaps may be revealed. This is to be expected, as developing the compliance program is a discovery process that will help the institution see – and ultimately close – those gaps over time. Gaps are identified by doing a “residual risk assessment” (the level of risk remaining after
considering the design of controls in place) as part of this step.

The combination of the front-end (inherent) and back-end (residual) risk assessments described in both Step 2 and here can help institutions identify the most critical compliance components. This can potentially eliminate some work by focusing efforts on the most important compliance requirements, thereby reducing some scope. In addition to identifying gaps, the residual risk assessment process is also an important step in evaluating control design and setting risk appetite or level of risk acceptance related to each compliance component.

Coach the functional area to develop a realistic timeline for addressing gaps based on the severity of sanctions and risk ratings for the gap areas discovered. This, too, should be documented as part of the compliance program.

Again, it could take several years to capture all the elements of compliance from the many functional areas of the university onto the spreadsheet or a database. Once this is done, however, the spreadsheet or database can be made available on an easily accessed website as a reference for the entire user community. To enhance readability, spreadsheets can even be converted to a book-like format, with a table of contents organized by regulation that allows users to jump to areas of their interest.

5. Evaluate and audit – This step takes place after the others have been established for any given functional area. Depending on the extent of compliance requirements and the culture of the university, this can take up to several years to complete for all functional areas, but that is to be expected.

This step involves two stages. The first stage, evaluation, focuses on closing any gaps that still exist within a functional area – bringing the gaps to the attention of the compliance area owner and determining the best means of addressing the gaps, whether through new control processes, a task force to evaluate next steps, system enhancements, or other means.

The second and most advanced stage of this step occurs after all elements of the compliance program for a functional area are documented and most gaps addressed. At this time, IA can begin to determine if compliance owners are effectively overseeing practices to educate and ensure compliance in their areas through audit testing, as it is not until actual audit testing has been completed that the operating effectiveness of compliance controls can be determined to be adequate. If testing reveals too many exceptions, the effectiveness of the controls is essentially inadequate and at least one of two things needs to occur:

1. The control design needs to be re-evaluated and changed to reflect what should happen (because testing revealed that the control does not really meet the control objective), or

2. The person(s) responsible for performing the control may need additional education to remind them that the control needs to be performed correctly.

CONCLUSION

The amount and complexity of regulation and the need for compliance adherence in higher education will continue to grow. Compliance failures in higher education have been receiving more attention, and the consequences have become prohibitively expensive. Universities need a means to protect against these consequences.

Given that IA has an obligation to help the organization improve governance and controls – and auditors possess the skills to systematically develop work plans to capture and document information across the institution, especially in areas related to controls and monitoring – it makes perfect sense for IA to drive development of a university’s compliance program effort.

The five-step process described here makes it relatively easy to begin implementing a program. If your institution does not yet have a compliance officer or compliance program, consider it IA’s professional responsibility to suggest to management that IA drive the program to ensure proper processes are in place and documented to achieve compliance.

ENDNOTES
1. For more information, see Protiviti’s Internal Auditing in Higher Education, available at www.protiviti.com.
Electronic Workpapers (On the Cheap)

By Mel Hudson-Nowak, MBA, CIA, Internal Audit Practices Section Editor

In small audit shops, comprehensive audit software is an unaffordable luxury. A handful of auditors work with what they have on hand … shared drive space, word processing documents and spreadsheets … and rely on tribal knowledge and easy communication to keep workpapers compliant and connected.

A new solution is emerging between comprehensive audit software and loose leaf documents on a shared drive. A Microsoft software program called OneNote provides workpaper documentation that is collaborative, flexible, easy to use and cost-effective. This article provides a basic overview of the functionality of OneNote and how it can be used effectively as an electronic workpaper system that will not break even the skimpiest department budget.

COLLABORATIVE
One of the core advantages to audit software packages is the ability to maintain a single set of records that are accessible by the entire audit team. When you create a new OneNote file (called a “notebook”), the set-up wizard asks who will be using the file. Selecting the option to share the notebook on a server defaults the synchronize settings to ensure that changes made by one member of the team are recorded and that multiple changes are merged. Settings can be adjusted to allow off-line copies of the notebook to be maintained and then merged when reconnected.

Notebooks can be used to share a variety of useful information across the office. In addition to creating a notebook for each audit completed, notebooks can be used to maintain a department’s audit manual, to archive training materials and to store templates. Because multiple notebooks can be open at once, a user can simultaneously work on an active audit, reference the audit manual and pull down a workpaper template.

Unlike comprehensive audit software, OneNote does not provide access control restrictions or the ability to electronically approve workpapers in the system. While it is possible to restrict access to an entire notebook through its server setting, or to password protect particular sections using settings within OneNote, access control and change tracking ability is much more limited than in complex audit software. Specifically, the typical workflow for document creation and approval (i.e., the auditor create the workpaper and submits it to the manager who reviews and approves it) does not exist within OneNote. Compensating manual controls, like inserting scanned images of signed approval pages, may be utilized to document management approval.

FLEXIBLE
OneNote is remarkably flexible, allowing for a range of documentation options. Notebooks are organized with section tabs (across the top) and pages (down the side) so that audit teams can organize their audit programs and workpapers in a structured manner. A typical audit may include section tabs for the audit program, workpapers, regulatory reference and query design, with a page within the workpaper section tab for each workpaper created. (See Graphic 1)

Another surprise is how well OneNote supports both free form and structured documentation. In a typical audit, the process of collecting and documenting information can vary greatly from the planning stage to the fieldwork stage.

Free Form Documentation
During the planning stage of an audit – particularly an audit that hasn’t been completed in the past – a vast array of information is collected. The purpose of planning is to identify how a process is intended to work and what inherent and observed risks may impact success. Planning may be very structured for recurring audits but may vary significantly for other reviews.

The ‘blank canvas’ feel of OneNote is uniquely suited to planning. As auditors complete preliminary interviews or do background research on the process, they are able to work independently and link their workpapers back to the audit. With a few quick steps, an auditor can:

• Create a new planning page
• Insert a screen print of a university policy located on the website
• Highlight key passages
• Create a flow chart or insert a scanned flow chart written during the meeting
• Add a text box to suggest audit program steps to be considered
• Link the box to an index of potential steps for review at the next team meeting.
At BGU, we originally utilized OneNote for planning because it was much simpler and more flexible for handling the constant influx of new information we experienced in planning. We later learned that OneNote was also able to handle the formalized structure and systemic nature of fieldwork equally well.

**Structured Documentation**

Once planning has helped us to define the process and identify the key risks to be tested, a more formal structure is important. No matter how audit functions organize their audit program, all programs will involve specific tests that should be conducted and documented in a consistent manner. That consistency helps ensure that an independent reviewer will be able to replicate the testing process and reach the same conclusion.

OneNote does a good job of creating standard table-based templates (see Graphic 2) that can be used to direct auditors to complete certain information for each audit program step or critical fields in each workpaper. With the ability to link back to an audit manual, key standards (like the standard choices for the workpaper conclusion field) can be referenced real-time. However, OneNote cannot require fields to be completed or provide pre-defined selections in the same way a stand-alone audit application can. As an auditor might say, controls over complete and standardized workpaper development are directive, not preventative, and additional detective controls (to identify poor performance) will be necessary.

**EASY TO USE**

A key benefit to utilizing the OneNote tool for audit documentation is the ease of use. Staff members who have a good skill-level in other Microsoft Office applications (i.e., Word, Excel, PowerPoint, Outlook) will find that the menus and options are familiar.

New users in OneNote are provided with a standard notebook called “OneNote 2007 Guide.” The guide gives users two things. First, it contains useful information that can be reviewed prior to creating a notebook or can be referenced when questions arise. Second, clicking through the notebook provides initial comfort with what can be expected. Every page that is reviewed makes the interface feel a little more normal. The fact that the help is embedded within the tool, and not a pop-up window, is illustrative of OneNote’s functionality.

Additionally, the Office applications are intended to interface with OneNote. In the Outlook inbox, an icon on the main toolbar allows for an email to be instantly sent (with both text and attachments) to the default OneNote notebook. A button appears in any meeting notice in Outlook to create a link to meeting notes. A new OneNote page is created with a link back to the meeting in Outlook allowing a real-time reference.

When the application does not allow built in connectivity between related files, creating those connections manually is just as easy. Users can choose to create a hyperlink to a file stored in a different location or embed the file directly in the notebook. And although both options have benefits and risks, the ease by which the technology can hold audit documents together is remarkable.

<table>
<thead>
<tr>
<th>Benefits</th>
<th>Risks</th>
</tr>
</thead>
</table>
| Hyperlink to Saved File | • Users access file directly.  
| | • Link always references the most up-to-date version.  
| | • If the file is moved or deleted, the link won’t work.  
| | • Must manually update or redo link for changes.  
| Embedded File | • File becomes a part of the OneNote document.  
| | • Standard “double-click” opens file, saves incorporated.  
| | • User could incorrectly make changes to the file outside of OneNote.  
| | • Inability to search for the file in a directory.  

**COST EFFECTIVE**

Many organizations already have site licenses for Microsoft Office. OneNote is included in Office Home and Student 2007 and available as a stand-alone product for less than $75. For offices that would never be able to afford the installation and maintenance costs of comprehensive audit software, an investment of zero or even $300 for a team of four might be a worthwhile expenditure.

**THE BOTTOM LINE**

Microsoft OneNote provides a unique set of features that are a good match to audit documentation needs. As a collaborative, flexible, easy to use and cost effective tool, it should be considered by any audit office struggling with their current set-up. Auditors are quick to find instances where operations are less effective and efficient than they should be – this might be a place where looking objectively at your own process would reveal an opportunity for improvement. ■
ABOUT THE AUTHOR

Professor Marianne M. Jennings is a member of the Department of Management in the W.P. Carey School of Business at Arizona State University and is a professor of legal and ethical studies in business. At ASU she teaches graduate courses in the MBA program in business ethics and the legal environment of business. She served as director of the Joan and David Lincoln Center for Applied Ethics from 1995-1999. She has done consulting work for law firms, businesses and professional groups.

Professor Jennings has authored hundreds of articles in academic, professional and trade journals. Currently she has six textbooks and monographs in circulation. “A Business Tale: A Story of Ethics, Choices, Success, and a Very Large Rabbit,” a fable about business ethics, was chosen by Library Journal in 2004 as its business book of the year. “A Business Tale” was also a finalist for two other literary awards for 2004. Professor Jennings’ book on long-term success, “Building a Business Through Good Times and Bad: Lessons from Fifteen Companies, Each With a Century of Dividends”, was published in October 2002 and has been used by Booz, Allen, Hamilton for its work on business longevity. Her latest book, “The Seven Signs of Ethical Collapse,” was published by St. Martin’s Press in July 2006. Her books have been translated into five languages.

All the Cash, Much of the Risk, But Too Few of the Curbs

By Professor Marianne M. Jennings

There is a certain smugness from the academic ranks as we watch the Wall Street debacles with clicks of the tongue and shakes of the head. “Greed,” we posture. “Fundamental lack of a moral compass,” we diagnose. But if we allow our eyes to wander down a bit on the front pages we find that the academy has had a parallel path of its own peccadillos. A few of the missteps, from just the past year, include:

- Yale University agreed to pay $7.6 million to the federal government to settle allegations that researchers had engaged in grant accounting practices that should cause every institution to research its own grant practices. The first series of allegations dealt with researchers transferring unused grant funds at the end of grant periods. The federal rule is that unused funds at the end of the grant period must be returned to the government. Ah, but rules have loopholes, and Yale was accused of transferring those funds to other grants before the curtain went down. The second practice where the U.S. Attorney in Connecticut focused their attention was with faculty who were paid 100% of their salaries in the summer, using grant funds. The faculty activity reports, as signed, indicated that faculty members were working 100% (effort) on research activities. However, investigators found faculty were not performing 100% research during the summer months. The reported faculty members were not devoted exclusively to the grant research, despite being paid as if they were. The interesting justification for the common practice was that faculty cannot get paid by Yale in the summer, unless they are doing research, ergo, the uptick to 100%.1

- Weill Cornell Medical College researcher, Dr. Claudia Hensche released groundbreaking work on lung cancer in 2006 through the publication of her research in the New England Journal of Medicine. A footnote in the article indicated that nearly all of the $3.6 million in funding for her research had come from The Foundation for Lung Cancer: Early Detection, Prevention, and Treatment. However, a front-page New York Times story in 2008 revealed that nearly all of the funding for the Foundation had come from The Vector Group, the parent of Liggett Group, a cigarette company. The Foundation was headed by Dr. Hensche, with a board comprised of colleagues from Weill as well as directors of the college’s board.2 A 2009 Wall Street Journal article found another wrinkle in the Hensche research, which concluded that regular screening with a tomography machine could yield quicker diagnosis and better treatment. The Journal found that Dr. Hensche and a co-author on the lung cancer research received royalties from General Electric, a maker of tomography machines. Dr. Hensche said that she disclosed the royalties to the NEJM but that the board declined to disclose them in 2006. A 2008 NEJM correction disclosed the royalties.

- Heather Bresch, the daughter of Governor Joe Manchin of West Virginia, was made chief operating officer of Mylan, Inc. The chairman of Mylan is the largest benefactor of West Virginia University. Ms. Bresch is a long-time business associate of the then-president of West Virginia University. The press release covering Ms. Bresch’s promotion to COO indicated that she had earned her MBA from West Virginia University. WVU’s registrar pointed out that Ms. Bresch had earned 22 of the 48 credit hours required for her degree, but that she had not earned her MBA. A panel, without discussing actual courses taken or providing a rationale, recommended that she receive the degree retroactively.3 The provost acted on the recommendation and granted Ms. Bresch her degree. Amidst protests and votes of no confidence, the provost resigned. Eventually, the president, who would not revoke the retroactive degree even after the provost’s departure, also resigned.4

- Dr. Joseph Biederman, a prominent child psychiatrist, failed to disclose $1.6 million in income he had received from pharmaceutical firms, a violation of both Harvard University and federal research policies and regulations.5

Apart from the obvious similarity that these were all Section One/Front Page stories, there are some important common threads that reveal lapses in policies, internal controls and ethics. Colleges and universities face similar bottom-line pressures that exist in business. The funds in higher education are flowing, from government grants, revenue and donors. There are pressures to gain and retain positions in rankings. Finding legislative favor has
higher education lobbyists and administrators firmly planted in the halls of state legislatures. We are indeed running major businesses … complete with all the temptations.

However, the nobility of the purposes and goals of higher education should not blind us to our vulnerability to lapses, because of these pressures and, perhaps unwittingly, because of lax processes and, too often, an absence of internal controls. Herewith some suggestions and lessons gleaned from these highlighted case studies.

**THESE WERE NOT CLOSE CALLS**

The situations noted carry neither the emotion of the classic Les Miserables theft of bread by a starving youth nor the complexity of an issue such as when life begins. These examples involve colleges, universities, administrators, and professors in clear violation of existing standards, rules and even laws. We read these examples and have a question similar to the one that appeared on the cover of Fortune magazine when we learned that Merrill Lynch had lost $55 billion, Bear Sterns was bankrupt, Lehman could not survive, and AIG was reeling: “What Were They Smoking?”

General Electric had criminal difficulties for its time-card fraud scandal when employees were falsifying their time cards to transfer their work to government projects where there was money left for pay. The researchers in this article’s opening examples were transferring funds among and between grants to save the last of the funds. Not to put too fine a point on the discussion, but the researchers were falsifying government paperwork, known in corporate circles as fraud. The same is true of their affidavits of 100% activity.

For the Harvard psychiatrist and the Cornell researcher, there is a classic conflict of interest. There are only two ways to resolve a conflict of interest: don’t do it or disclose it. Neither did either in their work. Indeed, Dr. Biederman’s press release indicates a fundamental misunderstanding of conflicts of interest and why we worry about them, “My interests are solely in the advancement of medical treatment through rigorous and objective study.” Dr. Biederman may well be the finest child psychiatrist on the planet, those abilities exceeded only by his absolute integrity. Dr. Biederman still has a conflict of interest and all payments should have been disclosed.

The lessons and application here are quite simple: Train university folks early and often in rules, policies, procedures and ethics. One portion might be a rule as simple as, “We don’t award degrees unless the course work has been completed. Any special committees, discussion, or retroactive awards are subject to review by the ______________.”

Part of that ethics training should also include examples such as these, so that those in the academy can internalize and apply them to their own unfolding situations. Ethics training should have as its purpose the instilling of discomfort. In other words, those in the training session should walk out, indeed run out, prepared to make changes in current procedures that simply may reflect complacency or laxity. Reminding folks that even the mighty have fallen has a way of stirring them into action and self-correction.

**THE STAR FACTOR**

Management research in business indicates that we have different standards for stars, i.e., those who are rainmakers or are able to expedite project completion to exceptional levels. If a mediocre employee crosses an ethical line or two, we are at the ready with enforcement and sanctions. When stars bend rules, we are reticent, deferential to them, their careers and the flow of funds that they keep coming. Those who discover ethical or legal missteps by stars are hesitant to take action. Our examples illustrate that we have two choices: (1) We can take action, resolve the misstep, self-report, and enjoy the credit that comes with that self-regulation; or (2) We can wait for the headlines that not only reveal the missteps but also bring into question the quality of operations and internal controls. Without action against the stars that cross those lines, we create a culture in which more employees, throughout the organization, will become emboldened and blur even more lines.

Part of the star factor can also be the “connectivity factor,” those involved in the misstep are well connected and can help the college or university, as in the situation with the governor’s daughter and her position with a company that was important to the university as well. Again, these signals of preferential treatment are poison to an ethical culture. At one university, a staff member from residential life asked this writer about a situation she found troubling. A young man who wanted to move out of the dorms did not qualify for one of the exceptional circumstances the university allowed students to use for ending their residence contract without penalty. The residential life administrator required the young man to pay his $700 fee to end his dorm contract. Shortly after she had made the decision and told the student, she received a call from a vice president who said, “His uncle is a really important donor to the university. Isn’t there something you can do?” How important could the uncle be as a donor if he can’t ante up the $700 to help out his nephew? Bend the rules for connectivity and you create a culture in which no one is sure what the rules are or when and if they apply. If a staff member awarded a contract to a family member, that staff member would be disciplined. But fixing a dorm contract for a major donor is different? The inconsistencies in treatment of employees causes confusion and rules then blur.

The fix for stars and connectivity is to be sure that staff members who are faced with these situations...
and who must correct a prominent researcher on paperwork or conduct, have support. However, often the staff member is functioning in a cluster in which the star has control. The time has come for all colleges and universities to move beyond ombudpersons to ethics and compliance officers. Without this independent office, with funding and authority, the lapses and missteps explained here will continue. Ethics officers and offices have been around military contractors for two decades and exist in 90% of publicly traded companies. The pioneering work on their creation and operation has been done and can be built upon when implementing a compliance and ethics function in colleges and universities.

**IMPLEMENT SOME CHECKS AND BALANCES**

In each of the situations described, the question most of us have is, “How many people had to know about this?” In the Cornell example, we had administrators, board members, and faculty serving on the very foundation whose funding was kept secret in research publications. In the Yale example, think through the number of people who are responsible for reviewing, filing, and submitting grant paperwork. The stars did not act in isolation. At West Virginia University, there were committees of faculty members who reviewed the program of study and the deficiency in credit hours.

However, what is clear is that there were not enough independent eyes looking at the researchers, the committees and their decisions and actions. Auditors play that role. But there is room for more. There is a reason academics have someone outside the major department serve on thesis and dissertation committees. The outsider provides the checks and balances for shoddy work that might be passed through because of department or college politics. Grants and even the consulting forms of faculty do not have enough independent evaluation to check for the missteps of excessive compensation or even just the pattern of all grants being zeroed out through transfers. Going through the specifics in these cases could provide a checklist of processes to conduct differently to attain that independence. Colleges and universities are not immune. Take these examples. Use them for training. Learn from them. And then implement the changes to prevent them, or, at a minimum, catch them before they make it to the front page.

**ENDNOTES**

Medical Records: Signed, Sealed and Secure
By Kay Hardgrave, CPA, CFE

As patients are diagnosed and treated in University hospitals and clinics, the Health Information Management (HIM) department collects and stores information about each patient through use of medical records. The HIM is responsible for coding, transcribing, maintaining and protecting the medical records of all patients. Accuracy, completion and timeliness of medical records directly impacts medical decision making and accuracy of billing. Access to the records 24 hours/7 days a week adds to the complexity. Unauthorized access to records with Protected Health Information (PHI) increases privacy and security risks and potential non-compliance with the Federal Health Insurance Portability and Accountability Act (HIPAA). The above may result in penalties and negative publicity. Additionally, medical identity theft is on the increase. For all these reasons, the safeguarding of medical records is critical.

The process of developing the medical records audit program should be risk driven – ideally, the result of a brainstorming session. See Table 1 for an example. Identify the applicable risks based on the background and scope. Consider the following:

- Are the medical records for patients in a hospital and/or clinics? Are the records housed in one department?
- Are the medical records primarily physical patient files, electronic medical records (EMR) or a hybrid? Many organizations will be in a hybrid state as they expand the use of EMRs. For example, radiology and lab reports, pharmacy and medical administration records may convert to EMRs, while the physician order entry system may still be physical.

This article focuses on an audit for a hybrid state of records, primarily physical charts. However, as hospitals and clinics convert to EMRs, the shift in audit risks will require you to go back and audit with different steps and related testing. Audit objectives include the following:

- Assess the overall general controls over the environment; and
- Evaluate the controls over physical security, procedures for release of records, third party contracts, timeliness of physician chart completion, and training.

Although transcription and coding accuracy and efficiency are important areas, this article does not address these except for a limited step for coding. The emphasis of the program below is compliance with HIPAA, contracts, policies and laws.

OVERALL CONTROLS AND PHYSICAL SECURITY
In order to assess the controls over the environment, especially security and privacy, it is important to conduct a walk-through and observe! Request a guided tour of every HIM location. In a hospital, an emergency room may have a satellite HIM location. Do not forget older records stored in the basement. During the tour, complete the developed checklist along with follow-up questions. If there are multiple locations, use a separate checklist for each one. Comparing the environment in various locations assists in identifying inconsistencies, procedures and conditions. See Checklist.

TESTS OF CONTROLS OVER SECURITY AND PRIVACY

1. Data regarding Physical Access – Badge System
How is management monitoring for suspicious activity regarding access? How do you know who has access, when, or the length of time spent in area after business hours? How do you verify the effective date access was terminated? Can a transferred or terminated employee use their badge to access the department, especially after-hours? Verify with the administrator of the University badge system how quickly an employee’s badge is deactivated and whether the employee has to turn in the badge for deactivation to occur. If the badge system is a stand-alone system and not integrated with the University badge system, how does deactivation occur? Obtain and review a report of access data. Compare data with the list provided by management of approved users and their access hours. Review list of users and dates of access; compare to terminated/transferred employees and effective date of termination/transfer, especially from the HIM department.

2. Follow the Records – Test how patient privacy is maintained during transport of medical records
Identify the general routes and procedures for physical records that are in transit – either collected...
for HIM or sent from HIM to another location; e.g., delivered to a clinic. Are records transported within HIM because a functional area is physically in another area; e.g., coding or transcription?

Accompany staff members on routes and observe practices to protect patients’ privacy from prying eyes. Do they consistently cover the records? Are loose records carried in their hands, or in an uncovered cart or bin? If they are being carried through a facility, can someone read patient information such as social security numbers, medical procedures, and even patient names if he is standing close in an elevator? If a vehicle is used, are windows tinted or passengers prohibited?

3. Software – Information Security Assessment

Identify any subsystems that feed into and are integrated for the creation and tracking of the patient’s medical record. Ask your IT department to assist with an information security assessment on software that is used by HIM and/or other departments for medical records. Some of the questions may include:

- Are inactive user IDs deactivated?
- Are the audit software controls turned on? Are audit logs reviewed?

4. Tests of Filing Accuracy

Select a sample of patient files; test for misfiled protected health information – the inclusion of another patient’s medical record.

Select a sample of medical record numbers from populations of patients discharged and patients recently admitted, to determine the recorded location of the record. Test if the record can be located quickly at the first attempt. If it is a physical file, observe the pulling of the chart. If it is in HIM, could the staff locate the file on the first attempt? If it is out on a hospital floor, could it be located quickly at the nursing unit? If an electronic medical record, observe the staff utilizing the software to retrieve the record.

Select a group of files. Determine if they are filed per department standards; e.g. physical files filed by last four terminal digits.

**PROCEDURES FOR RELEASE OF INFORMATION (ROI)**

Copies of medical records are requested from external groups – patients and attorneys – as well as internal requests from the denial of claims (appeals) staff and patient billing services needing records to seek reimbursement. Determine whether the procedures are compliant with HIPAA and any state laws that govern the rates charged for the copies. Determine if the Release of Information (ROI) function is handled in-house or if it has been outsourced. If outsourced, see section on Third Party Contracts.

Tour the ROI area and observe the following for HIPAA compliance:

1. Is there adequate privacy for patients?
2. Are required notices posted regarding HIPAA and complaints? Even if outsourced, the complaint notice should provide the name and phone number of the HIM director.

Inquire as to the performance of the area or current contractor. Have there been complaints from patients as to a delay in receipt of records that may result in patient dissatisfaction? Since the primary source of the contractor’s revenues is external customers, there may be delays in processing internal requests. Check with internal customers – denials and patient billing services – regarding the timeliness of responses. The delay in processing denials results in slower or potentially reduced reimbursement for services. Ask them for a report indicating the number of days outstanding for their requests and required follow-up.

Observe how the ROI staff handles the security and privacy of records in transit.

Cash Handling/Credit Cards – If payment is not the responsibility of third party contractor, then evaluate the controls. Also determine compliance with credit card policies to protect the personal information; i.e. the credit card number.

Review all third-party contracts with companies that access, review or perform functions with medical records for the following:

1. HIPAA training responsibility

<table>
<thead>
<tr>
<th>RISKS</th>
<th>RISKS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lack of physical protection of medical records</td>
<td>Incomplete record</td>
</tr>
<tr>
<td>Inability to locate a paper chart</td>
<td>Untimely filing of test results</td>
</tr>
<tr>
<td>Wrong patient’s information in another patient’s chart</td>
<td>Inadequate transcription services – may have errors or backlog</td>
</tr>
<tr>
<td>Disclosure of PHI without authorization</td>
<td>Maintenance of shadow charts by physicians</td>
</tr>
<tr>
<td>Inappropriate release of information</td>
<td>Hybrid of medical records (part paper, part EMR)</td>
</tr>
<tr>
<td>Lack of effective tracking of medical records</td>
<td>Unauthorized modification</td>
</tr>
<tr>
<td>Inappropriate access by staff</td>
<td>Ability to back-up and recover data</td>
</tr>
<tr>
<td>Lack of monitoring access to medical records</td>
<td>Storage of records on unsecured devices</td>
</tr>
</tbody>
</table>
Financial arrangement – Do the terms reflect the intent of HIM management with the third party as described to you? Is the university providing space? Are there revenue sharing or payment terms? Compare terms to invoices for appropriate approvals and accuracy. For example, a company providing ROI services may charge for internal requests, usually for the number of copies that exceed a threshold per month at a per page rate. Review invoices per page rate to contractual rate. If the company has overcharged a few cents more per page, the recovery amount can add up to thousands of dollars!

3. Does the contract require a quality assurance program to be in place? If so, review their procedures. For example, if a company is assisting with a backlog of filing loose paper, what is done to verify filing accuracy?

4. Standard audit clause

5. If there is a contractor that is not in a direct contractual relationship with the university, but
is reviewing patient charts as part of their duties, verify there is a Business Associate Agreement to cover their chart review for HIPAA purposes.

**TIMELINESS/DELINQUENCIES OF PHYSICIANS COMPLETING CHARTS**

To be in compliance, physicians must complete charts before patients’ bills are dropped; i.e., claims are filed for payment. What is the policy on deadlines? How are the timeliness or delinquencies of chart completion monitored by HIM? Is the staff proactive by sending physicians reminders that charts are incomplete? If so, review the number of days that lapse after the discharge date before reminders. How often do medical delinquencies occur? What are the enforcement practices for delinquencies?

**Training** – Are new employees HIPAA trained before they begin? Check training logs. Ask for documented desktop procedures and if additional training is offered.

**Coding** – Two quick steps regarding coding accuracy include:

1. **Emergency Room** – Does the HIM coder perform an independent reconciliation of the ER medical records against the ER daily patient log to ensure that the hospital has captured the charges to reimburse the hospital for its services?

2. **External Audit Reports** – If external audit reports are performed on the coding accuracy, review for the most current report’s results and recommendations. How does HIM follow up with the recommendations or if a coder has less than satisfactory performance? Has HIM presented the report to senior management and/or a compliance committee?

**CONCLUSION**

Internal Audit’s added value of an audit focused on compliance is to help ensure that medical records are signed, sealed and secure from inappropriate access. This will mitigate the risk of the university’s exposure to potential penalties and negative publicity.

The institution also requires annual management-level training and certification whereby anyone with account oversight must take on-line training and then certify that duties are being segregated and accounts are being reconciled.

**Monitoring**

The Compliance Office conducts some monitoring of high risk areas referred to as “inspections.” The purpose of these inspections is to make sure the basic elements of the management plans for each high risk area are in place and are functioning as intended. Inspections are not meant to replace the audit function. The audit function will provide the assurance that controls are working as intended subject to the annual audit plan.

In order to prevent duplication between the Audit & Compliance functions, the Audit Office generally will not perform an audit of a high risk compliance area until the risk assessment and management plans have been completed by the responsible individuals and the Compliance Office has conducted its inspection. At that point, the area is deemed “ready for audit” and can be included in the audit risk assessment and plan.

Finally, the University contracts with an outside provider for its confidential reporting mechanism. The details of the “hot line” call are received by the Compliance Office who determines which area most appropriately should handle the issue. The Compliance Office will investigate many of the issues. However, many issues will also be handled by Human Resources, Audit or the Public Safety department.

Both the compliance and audit functions perform important activities on our campus that maintain the integrity of our operating activities while attaining an effective compliance environment.

Please contact me at dick.dawson@utsa.edu or visit our website at www.utsa.edu/acrs with questions on this topic or any other ACUA issue.
Auditing: Understanding the Difference

By Andrea Claire, JD, MBA

At UT Southwestern Medical Center at Dallas, the Office of Internal Audit (IA) and the Institutional Compliance Office (ICO) both want the same thing: to add value and improve operations while providing assurance to senior administration of a well-managed, secure, ethical and compliant environment. The way these two offices achieve that objective is appropriately unique to their defined roles. The Institutional Compliance Office is part of management with a responsibility to promote a continuous and proactive compliance function. Conversely, the Office of Internal Audit is independent of management and has the responsibility to evaluate operations including the Institutional Compliance Office. Although their roles are different, both IA and ICO are in the risk game and both rely on each other as a resource.

The following article shares details of the UT Southwestern Medical Center at Dallas model.

**INTERNAL CONTROL STRUCTURE**

While audit and compliance have several role distinctions, a significant difference relates to the internal control structure. The Institutional Compliance Office (ICO) is a key component of the internal control structure at UT Southwestern, while the Office of Internal Audit (IA) is responsible for evaluating and reporting on the internal control structure. Specifically, the Institutional Compliance Program Plan is designed to assist the University in fulfilling its compliance responsibilities by creating an operational structure that outlines and documents the University’s compliance efforts (ICO website). An internal audit objective is to evaluate the adequacy of the internal control structure to manage risk (IA website).

**OPERATING STANDARDS AND ORIGINS**

The Internal Audit function is required by the UT System Policy UTS129: Internal Audit Activities and was mandated by the Texas Internal Auditing Act, (TX Govt. Code Ch. 2102). Internal Audit follows the Institute of Internal Audit (IIA) standards when conducting audits. The IIA Standards for the Professional Practice of Internal Auditing (Standards) provides guidance for the conduct of internal auditing at both the organizational and individual auditor levels. These standards include requirements such as: independence and objectivity, proficiency and due professional care and a quality assurance and improvement program.

**OVERSIGHT COMMITTEES**

Institutional Compliance oversight committees include the: Executive Compliance Committee, Institutional Compliance Advisory Committee, and Billing Compliance Committee. The Internal Audit oversight committees include the: UT Southwestern Medical Center Audit Committee and the Audit, Compliance and Management Review (ACMR) Committee of the UT System Board of Regents.

**RISK MITIGATION**

Both Offices are in the business of identifying and mitigating risks for UT Southwestern Medical Center. While the process is different, IA and ICO each conduct annual risk assessments. For each...
<table>
<thead>
<tr>
<th>Summary of Responsibilities</th>
<th>Institutional Compliance Office</th>
<th>Office of Internal Audit</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Internal Control Structure</strong></td>
<td>Key component of internal control structure</td>
<td>Evaluates and reports on internal control structure</td>
</tr>
<tr>
<td><strong>Assurance Work</strong></td>
<td>Compliance</td>
<td>Compliance • Financial • Operational • IT</td>
</tr>
<tr>
<td><strong>Report Distribution</strong></td>
<td>Members of the Executive Compliance Committee comprised of the University President and other members of executive management</td>
<td>Department Management, Executive Management, UT Southwestern Medical Center Audit Committee, UT System Internal Audit, UT System quarterly report summary to the Board of Regents, Governor’s Office, the Legislative Budget Board and the State Auditor’s Office</td>
</tr>
<tr>
<td><strong>Oversight Committees</strong></td>
<td>• Executive Compliance Committee • Institutional Compliance Advisory Committee • Billing Compliance Committee</td>
<td>• UT Southwestern Audit Committee • UT System Audit Committee</td>
</tr>
<tr>
<td><strong>Other Services</strong></td>
<td>• Compliance plans • Ongoing monitoring • Online Compliance Training • Compliance Newsletter • Standard of Conduct Guide • Ethics Line triage and referrals to IA, HR, etc.</td>
<td>• Consulting services • Investigative Audits • Internal Controls Training</td>
</tr>
<tr>
<td><strong>Risk Mitigation</strong></td>
<td>• Annual risk assessment to identify critical compliance risks • Monitor risks identified</td>
<td>• Annual risk assessment to prepare annual audit plan • Audit risks identified</td>
</tr>
<tr>
<td><strong>Joint Compliance Work</strong></td>
<td>Assurance reviews of compliance</td>
<td>Audits of compliance</td>
</tr>
</tbody>
</table>

Critical compliance risk identified by ICO, a compliance monitoring plan is developed to ensure that all critical compliance risks are monitored. Internal audit assesses risks to ensure that the highest risk areas receive coverage on the annual audit plan.

### TYPES OF ASSURANCE WORK PERFORMED

Institutional Compliance performs compliance assurance reviews for each department which are similar to compliance audits performed by internal audit. In addition to compliance audits, Internal Audit performs financial, operational and information technology audits.

### REPORTING

Internal Audit reports are distributed to Department Management, members of executive management including the University President, and UT System Internal Audit. Internal Audit reports are also presented to the UT Southwestern Medical Center Audit Committee and to the ACMR Committee of the UT System Board of Regents. In addition, copies of reports are required to be distributed to the Governor’s Office, the Legislative Budget Board and the State Auditor’s Office.

Institutional Compliance reports are distributed to members of the Executive Compliance Committee which is comprised of the University President and other members of executive management. A summary compliance report is distributed to UT System quarterly and annually.

### OTHER SERVICES PERFORMED

Other services performed by both offices vary greatly. The Institutional Compliance Office (ICO) assists departments to develop risk-specific compliance plans, and the ICO conducts ongoing evaluations and monitoring activities on a routine basis. The ICO also provides online compliance training and monitors employee completion of required training. The ICO reviews all Ethicsline complaints and determines which to refer to Compliance, Human Resources or Internal Audit. The quarterly compliance newsletter and employee standard of conduct guide are also prepared by the Institutional Compliance Office.

Internal Audit (IA) performs certain other activities in addition to the previously mentioned audits. IA performs consulting services to management and investigative audits initiated from requests by department personnel, administrative management, the public safety department, ICO, etc. Additionally, Internal Audit provides training to departments in areas such as internal controls.

### CERTAIN COMPLIANCE WORK MAY BE PERFORMED JOINTLY

Assurance reviews are conducted by ICO on an annual basis to ensure that all critical risk compliance activities are functioning as designed in the monitoring plan. Assurance reviews may be conducted jointly with Internal Audit when an audit of that risk area has been scheduled.
Addressing Common Barriers to Using CAATs

Advantages of Putting Technology to Work on an Audit

By IT Guest Columnist Donald E. Sparks, CIA, CISA, ARM

Change can be difficult for anyone. Inventor Charles Kettering once said, “The world hates change, yet it is the only thing that has brought progress.” We should keep these words in mind when it comes to considering whether to move beyond the tried-and-true methods of manual auditing towards Computer Assisted Audit Techniques (CAATs) and the use of data analysis software.

Although CAATs have been around for more than 25 years, they have only recently become common practice. By our nature, most internal auditors are inclined to stick with what has “worked just fine” in the past, rather than reach outside our comfort zone for an alternative that could help us accomplish more. What we should be asking ourselves is, “Could we do something electronically in 20 minutes that would normally take us 20 hours, and possibly improve the quality of our work as a result?”

Since most organizations use computer systems extensively, it is nearly impossible to conduct an audit without using technology. In fact, the AICPA issued new rules in 2008 stating that testing journal entries must be done electronically. Audit standards are starting to advocate the use of CAATs, and for good reasons. Using CAATs and data analysis tools allows auditors both to view high-level business operations and to drill down into the data. They can also be used to identify anomalies, which may lead to the discovery of errors and fraudulent activity. While technology may be used to improve the audit and reduce the time necessary to complete the engagement, some auditors may still be reluctant to make the switch.

Knowing Your Limits

The volume of data has increased significantly in the past few years. Most data analysis tools allow an auditor to extract an unlimited number of files. By comparison, traditional tools such as spreadsheets can handle only a certain number of rows. The actual row capacity depends on which version is used.

In today’s fast-paced environment, some auditors must review databases containing several million lines in order to detect anomalies. Identifying anomalies, to include missing entries, is essential to pinpoint errors and fraud exposures within multiple units of a complex organization. It is virtually impossible to review that amount of data manually and be assured nothing was missed or that all potential exposures were identified. Data analysis software allows the auditor to find things one would not normally see simply by flipping through pages of data or scanning millions of lines of information.

CONSIDER THE RISK

CAATs and data analysis tools allow the auditor to question things at a different level and see things which would not normally be caught. Such capability is critical considering that auditors are counted on to find anomalies, errors and fraud no matter how great the volume of data.
Spreadsheets can be used for certain tasks, but they do not allow others to track and follow which tasks were performed. Using CAATs, an auditor can link a history report to a sample and prove it was a stratified random sample — something that typically cannot be done using a spreadsheet. The auditor can also verify that the entire population was captured and ensure that 100 percent of the transactions or entries were reviewed.

Auditors must exercise caution when using spreadsheets because there may be no way to ensure the data are fully protected. Moreover, spreadsheets may not provide the necessary documentation required to meet audit standards. Data captured in a spreadsheet can be accidently or purposely overwritten, whereas data analysis software ensures the integrity of the database by creating a copy.

**NOT EVERYTHING IS REPLACEABLE**

Data analysis software is not the answer to everything, but it can serve as a valuable tool to achieve an objective. For example, such software cannot take the place of the brainstorming phase during which the audit team determines which account balances and transaction cycles are significant and material. However, data analysis software can be very useful in planning analytics and determining that nothing was missed. Once the right account balances and transaction cycles are determined, the auditor can use a data analysis tool to expand the scope of the analysis and increase audit coverage.

Additionally, while data analysis software can simplify data downloads and transfers by reading data in virtually any format, the auditor will still need to know the record layout and what specific data are in which fields of the records. The same is true for determining what needs to be verified and tested, which requires an auditor’s knowledge of the application, the organization and the risks.

Once an auditor realizes the value of the software and the areas where it can best serve the organization, the auditor will find that it brings greater efficiency and progress to audit work.
In today’s increasingly challenging business environment, organizations are looking to internal audit to take on the role of trusted advisors that provide ongoing assurance. Our technology provides the analytic capabilities to give you greater insight into key risk areas in your audit...

**confidence** in your results...

**freedom from doubt**
Can you foresee the consequences?

The consequences of overlooking, ignoring, or misjudging institutional risks are severe. Your hotline is an important tool for risk awareness, but forward-thinking institutions are looking beyond their hotline to develop a formalized view of a broader set of issues and events. EthicsPoint's comprehensive, on-demand solution, supported by our global hotline, provides an end-to-end framework for the awareness and management of issues and events across your institution.

For more information, visit www.ethicspoint.com