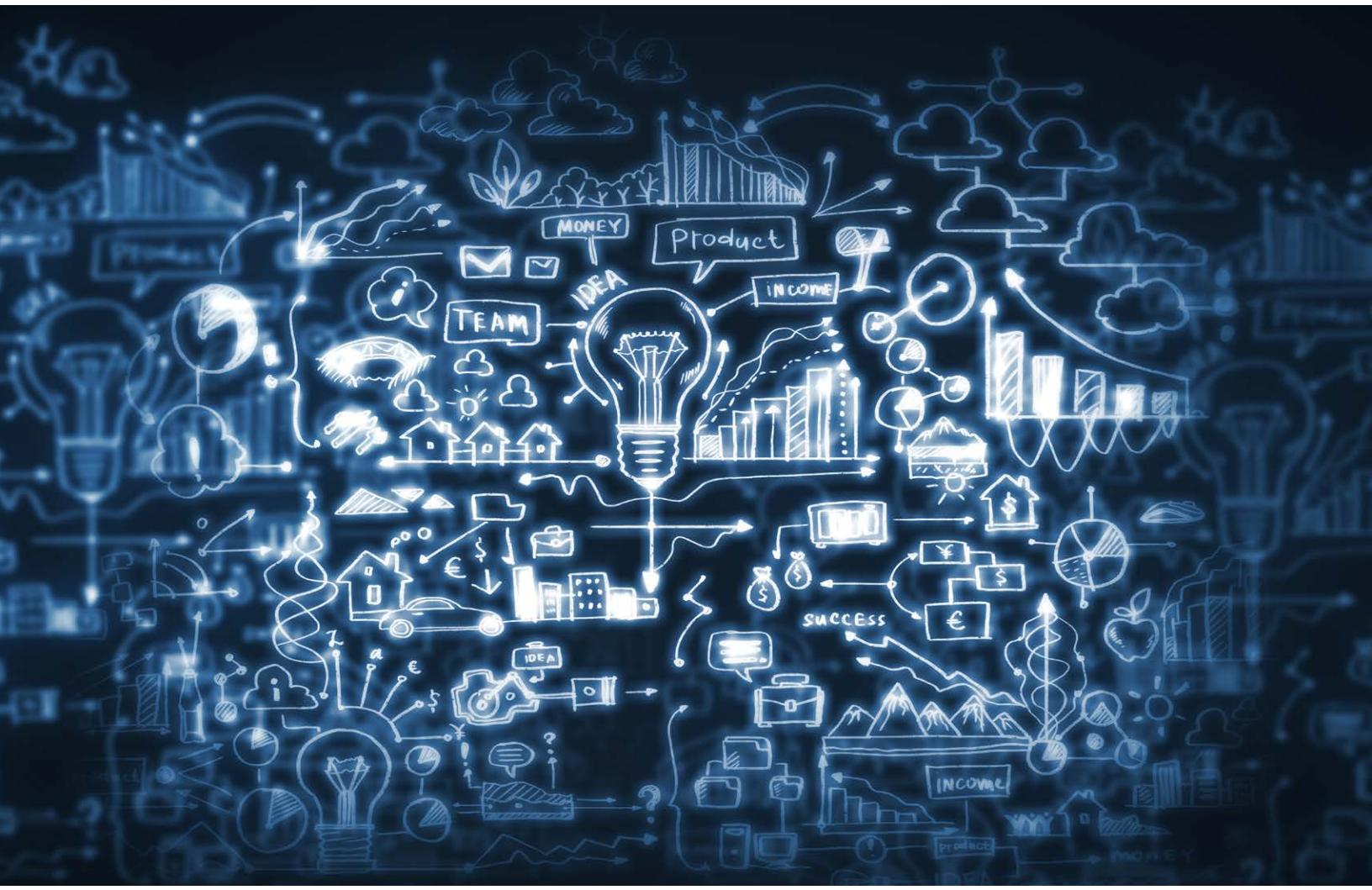
| VOLUME 56 | NUMBER 2 | SUMMER 2014 |

COLLEGE & UNIVERSITY AUDITOR



ACUA
ASSOCIATION OF COLLEGE & UNIVERSITY AUDITORS

INSIDE:

SUMMER 2014
COLLEGE & UNIVERSITY AUDITOR

CONTENTS

FEATURES

LEADERSHIP

AUDIT TOOLS

ENTERPRISE RISK MANAGEMENT

COMPLIANCE

COLUMNS

MEMBERS

DEPARTMENTS

ACUA members are invited to submit letters and original articles to the editor. Go to **www.acua.org** and click on the Resources – *College & University Auditor Journal* for further guidelines. The editor reserves the right to reject, abridge or modify any advertising, editorial or other material.

Send address changes to:
ACUA
PO Box 14306
Lenexa, KS 66285-4306
ACUA-info@goAMP.com

LETTER FROM

THE EDITOR

By Sam Khan
Editor

This is my first issue as *College and University Auditor*'s editor. I am honored to serve in this new role for the journal. During the previous year, as the deputy editor, I had the opportunity to work with and learn from our former editor, Clarice Maseberg. I hope to continue where she left off, by producing relevant and engaging articles that help us become more effective auditors.

I hope to continue where she left off, by producing relevant and engaging articles that help us become more effective auditors.

In this issue author Cathy McCullough walks readers through a six-step process to help turn a difficult situation into an opportunity for success in her column "How to Prepare for a Difficult Conversation."

In part 2 of Sterling Roth's "How Much is Higher Education Like a Business?" he shares results from his dissertation research in which he explores the views of 144 internal audit directors at U.S. research universities.

Author La Donna Flynn discusses the various risks associated with a student health center and provides an excellent guideline for an audit program in "Are You Auditing Your Student Health Center? If Not, Why Not?"

In our new IT column, "Network Security: 11 Questions Every Auditor Should Ask," author Allison MacFarlan formulates questions to ask security personnel to determine how well firewalls and intrusion detection/prevention systems are maintained. She points out that network and security personnel are expensive, therefore it is important to make sure they do their jobs well.

In "Putting the 'Enterprise' in Enterprise Risk Management," authors, Cheryl Lloyd, Carrie Frandsen, Emily Breed, Kimberly A. Newman and Erin Ann Thomas illustrate how the University of California has turned "Everyone is a Risk Manager" from a slogan to a reality. They continue to support user adoption of new risk management systems, enhancing processes and shaping behaviors in order to reach their goals.

Ensuring IT compliance with so many and often overlapping state and federal regulations can become a daunting task. In 2012, New Mexico State University took the first step towards tackling this issue when it created its IT Compliance Function and hired an IT compliance officer. Author Carlos S. Lobato talks about the challenges he faced and the achievements his function has made in "Managing IT Compliance Risk."

In a new column about small audit shops, Sonya von Heyking looks at the realities of life in a 'one-person audit shop' and gives pertinent advice about how to reduce stress and avoid burnout, which can be applied to a variety of scenarios, no matter the size of your audit function.

I want to thank all the people who helped make this issue possible. Volunteering for the journal is a great way to give back to the profession.

I encourage your feedback; letters to the editor are always a great means to voice your opinion. Additionally, please share topics that you would like to see covered in future issues. Feel free to call or email 541-737-7336 or sam.khan@oregonstate.edu. ■

LETTER FROM

THE PRESIDENT

By Doug Horr
President

Dear Friends and Colleagues,

As I am nearing the end of my term as President for this great organization, and this will be my final presidential "letter" to you, it of course makes me a bit reflective. Did we accomplish the goals I had in mind when I assumed the Presidency? Did I achieve the "engagement" I sought? Did we move the organization forward? What could I have done better? And maybe, and most importantly, did I do everything I could to ensure the next President (Sandy Jansen) had a solid foundation on which to build success?

Make no mistake about it, in our own institutions, we as managers and leaders are only as good as those people who work with us. Notice I said "with" and not "for." Because to truly lead a great organization, I believe you must first be willing to serve those you lead. How we train/develop our people, treat our people, and provide our people an environment where they can reach their true potential is the difference between just running another university department and managing a best in class function that the university relies on for success. We all have our own distinct strengths and weaknesses. Helping our people identify and overcome their weaknesses and synergizing their strengths is what an effective leader does, and how a department becomes great. This becomes even more apparent when it comes time for that leader to step down.

Make no mistake about it, in our own institutions, we as managers and leaders are only as good as those people who work with us.

As I look at the landscape of ACUA's institutional leaders, I recognize that many of those who have shaped this organization, and the profession, and who have mentored me and so many others, are near a time when they will be stepping down from their institutions (some already have). Many, I know, have planned for this in their audit shops. Their successors will rise from their organization's ranks and continue to build on the legacy created there, like most great organizations do. I would encourage all to think about what that means in your own institutions. What have you done to create that type of environment? Will you leave a foundation on which to build a better function? Have you helped develop or inspire future leaders?

Rest assured I have certainly thought about it. I pose the questions and not solutions because to provide a single answer is not feasible. How we each do these things depends on our own strengths and the environment in which we find ourselves. I only know they are questions that you should take the time to contemplate. I have learned a great deal from those whom I have been fortunate enough to serve you with, and I will miss this Board greatly. I can only hope that I have given the organization a fraction of what it has provided to me in terms of personal and professional growth, and that along the way I have inspired others to serve, or think a little about how to make their own organizations better. ■

Warm regards,

How to Prepare for a Difficult Conversation

By Cathy McCullough, M.S.

Internal audit leaders are faced with difficult conversations every day. Some struggle when talking to the less-than-productive employee or when delivering bad news to a client. These types of discussions are never easy. However, with proper preparation and with the help of this six-step framework, auditors can have the tools to turn a difficult situation into an opportunity for success.

Having difficult conversations isn't something most leaders are fully prepared to do. It is just easier to let it go. As a leader of people, recognize that a decision to let it go has implications such as lower morale, increased stress, decreased problem-solving ability, decreased productivity, inefficiency (other people will go to great lengths to work around difficult people versus having to work directly with them), increased turnover, and overall, lower results. Lack of performance due to difficult people costs you precious time, and they cost you money. Ultimately, everyone loses.

The people conversation will:

- iron out wrinkles of misunderstandings about who does what
- provide for the identification of clear and expressed expectations
- pinpoint where there are performance gaps
- establish a strong sense of commitment to high-performance
- give you a framework for how to measure each person's performance

According to Daniel Goleman in *Primal Leadership (2002),* how people feel about working at a company can account for 20 to 30 percent of business performance.

In the end, having a people conversation is the first step in confirming your leadership intent of creating a high-performance division or organization. The long-term benefits for your division, then, will be seen via streamlined decision-making, a stronger sense of decisiveness, and healthier departmental/organizational culture.

A SIX-STEP FRAMEWORK FOR DIFFICULT DISCUSSIONS

Unfortunately, most leaders simply want to make this conversation easy; as a result, they tend to gloss over real issues or talk in generalities rather than in specifics. The leader simply tells the person what to do because it seems easier, to the point, and faster. The bad news is that the simplistic approach will not change behavior, nor will it change the response. The following suggested framework will help guide your thinking as you prepare for and carry out a difficult conversation.

(1) Clarify Your Own Thinking

- What, specifically, are the problem behaviors? Within the full scheme of things, what impact are these behaviors having on the work environment? What would you, as the leader, like to see the person do differently?
- During this pre-thinking time, be sure to also get in touch with your own emotions about this situation. Are you angry? Frustrated? If you don't get your own emotions in check, you will stray from the facts of the situation, and your emotions will take over during the actual

ABOUT THE AUTHOR

Cathy McCullough, M.S., *principal of McCullough Group (www.MLeadershipGroup.com) and Executive & Corporate Coach for Gazelles Systems, Inc. (www.GazellesSystems.com), works with key leaders in organizations of all sizes and sectors relative to strategic intent, high performance, and executive coaching. She is a speaker at international conferences on the topics of leadership, strategy, corporate culture, and "people issues."*

conversation which may result in making you agitated and frustrated or may cause you to jump to conclusions or to speed up the interview in order to get through it. It is a paradox. The stronger your reaction to their behavior, the harder it is for the individual to change. The goal is to stick to the facts, **always**.

- Anticipate how you think the person will respond or react.
- Pre-plan a few relevant open-ended questions.
- Ask yourself: Have I helped create this problem? How? What might I need to do differently?

Having clarified your own thinking, you're ready to start the conversation.

Having clarified your own thinking, you're ready to start the conversation.

(2) Frame the Situation

- Describe the specific behaviors that are concerning you. Describe the behaviors as specifically as possible. Give an example or two to demonstrate what you mean.

(3) Share the Impact of these Behaviors

- What's the impact? Why does this matter?

(4) Build Personal Accountability

This phase is the most crucial step of the entire conversation.

- At this point in the conversation you want to engage the other person to be a part of the discussion. Avoid the tendency to tell the person what to do. Instead, help people think for themselves. Guide them to create solutions to the situation. By doing this, you also begin to build a culture of personal accountability.
- During this step of the process, you primarily ask open-ended questions. Open-ended questions put the ball in the other person's court and that person creates the solution rather than you simply telling that person what you need him/her to do. This is what teaches people to think. So at this point, the conversation becomes a dialogue with you asking questions and the person doing almost all of the talking. The questions you ask depend on the situation, but here are a few examples:
  - What might you do differently so that we can minimize the possibility of this happening again?
  - What might you do to make this client relationship stronger?
  - How can you better serve our internal customers?
  - What do you think needs to be done? What next steps might you suggest?
  - How might you best get me the information I need so that I'm not blindsided again in the future?

- 65% of performance problems result from strained relationships between employees.
- Without having difficult discussions, leaders can spend up to 35% of their time dealing with the fallout of ongoing disruption.
- Estimate the time that is wasted by people who are trying to work around a difficult person. Equate that wasted time to salary and you have the cost of this disruptive situation.
- Up to 90% of involuntary departures are the result of having to deal with a difficult person.
- The cost of conflict can be figured by calculating (per salaried employee) wasted time, loss of skilled workers, restructuring time & energy to work around a conflict vs. deal with it, lost work time, etc.

Daniel Dana

- During this phase of the conversation, your job is two-fold: (a) Listen and (b) Keep the person *focused*. They might try to blame things on someone else or say that the client or peer is just demanding and hard to work with, etc. Those things might be true, but the behavior still needs to be changed by the person you're talking to.
- Consider: I understand. However, we're not here to talk about how unruly the client is (or how incapable so-and-so is at their job). We're here to discuss what needs to be done so that… (repeat what you said in earlier steps, and then repeat your initial question).
- If the person becomes angry, politely face that fact. "It appears that this frustrates you; however, we need to talk through this as two professionals. My desire is for us to create a win-win solution

because this has to be resolved." Then, repeat your question. You need something to happen or to be done differently; don't apologize for that. It is what it is. Keep repeating your open-ended questions, which should eventually force a response. Follow-up to the person's responses with more open-ended questions. Be prepared; stay focused.

(5) Create Action Steps & Audit the Results

- This final phase of the conversation is designed to move toward solutions and to help the person create the changes relative to the specific behaviors which need to be altered. This includes target dates or timeframes for specific actions, follow-up meetings to discuss noted improvements or continued actions if necessary, etc.

(6) Clarify Your Role

- As you dive into the action steps that have been identified and agreed upon, clarify your role. For instance, "How can I be a resource for you?" or "If you have questions along the way, I'm here to help." Your job during this portion is to listen and affirm.

Whether you're having a difficult discussion with a peer, a direct report, or a client, dealing with difficult people is a dynamic fact of organizational life.

Whether you're having a difficult discussion with a peer, a direct report, or a client, dealing with difficult people is a dynamic fact of organizational life. Ignoring difficult people and the situations they create can destroy a team's morale, sense of unity, and productivity. By addressing difficult conversations, teams can become re-energized and more productive. ■

How Much Is Higher Education Like a Business?

Part 2: Exploring Internal Auditing Views on Culture and Measuring Achievement

By Sterling Roth, CIA, CPA

How much is higher education like a business? Could a partial answer be found in how higher education internal audit directors view culture and measuring achievement differences between the two? To that end, this article explores the views of 144 internal audit directors for U.S. research universities who responded to my dissertation[1] research survey sent to 283 such officials in late 2010.

My Part 1 background article in the Spring 2013 Issue of *College and University Auditor*[2] concluded as follows:

> Views of culture and measuring achievement differences between universities and a business might ultimately determine not only how but also whether internal auditing is used in the academy. Exploring these views may be more than new and challenging. It may also be consequential.

This Part 2 article summarizes and explores those views and more. The views, relationships, and descriptive information discussed may confirm the expectations of some and contradict those of others. That is okay. I believe consequences lie less in consensus than in understanding. Understanding how the academy works and gauges its success may, in fact, be essential to our own. Thanks to the 144 internal audit directors who responded, we can add to that understanding.

ABOUT THE AUTHOR

Sterling Roth, CIA, CPA *is the Chief Audit Officer at Georgia State University (GSU). He retired from the U.S. Air Force (AF) as a colonel in 1998, having served as Chief of Pacific Audit Region, Director of AF Financial Management Audits, Director of the Department of Defense Professional Military Comptroller School, and Chief Financial Officer for Air University. He worked for the University of Alabama System at Birmingham and in Huntsville before coming to GSU in 2003. In addition to a Ph.D. in Educational Policy Studies from GSU, he has an MBA from Michigan State University and a BSBA from the University of North Carolina at Chapel Hill, both with an accounting major.*

CULTURE AND MEASURING ACHIEVEMENT VIEWS

How Different? The survey asked each director whether his or her institution's culture and a business's culture were "not at all different," "somewhat different," "very different," or "completely different" and the same regarding measuring achievement of his or her institution's missions and measuring achievement of a business's objectives.

> **Note:** Research, teaching, and public service missions are fundamental to a research university; profit and going concern objectives are fundamental to a business. Thus, the measuring achievement comparison was based on what was fundamental to each.

The most common choice for culture was very different, as 73 respondents or 51% made that choice, and for measuring achievement, somewhat different, as 55 respondents or 38% chose it.

In culture and measuring achievement, how different are your institution and a business?

	Not at all	Somewhat	Very	Completely
Culture	8 (6%)	55 (38%)	73 (51%)	8 (6%)
Measuring achievement	38 (26%)	55 (38%)	41 (28%)	10 (7%)

Businesslike or Distinct?

I combined the four categories into two: "not substantially different" (not at all or somewhat different) and "substantially different" (very or completely different), and then relabeled them "businesslike" and "distinct" from the institution's perspective. Using those terms, a majority of respondents, 56%, viewed their respective institution's culture distinct, and a larger majority, 65%, viewed its measuring achievement businesslike. Yet proportions holding opposite views were substantial: in both cases, over a third of respondents.

Inferred views of institution's culture and of how it measures achievement of its missions.		
	Businesslike	**Distinct**
Culture	44%	56%
Measuring achievement	65%	35%

Culture and Measuring Achievement Views Were Related

There was a statistically significant relationship between respondents' views of culture and their views of measuring achievement, with medium effect size or strength.[3] In fact, over two-thirds of directors viewed culture and measuring achievement the same: 38% viewed both businesslike; 30%, both distinct. Yet over a fourth, 26%, considered culture distinct and measuring achievement businesslike.

CHARACTERISTICS OF DIRECTORS AND INSTITUTIONS

Influencing Factors.

Finding factors possibly influencing these views led to further testing that included director and institutional characteristics, which are described next.

Directors' Characteristics

Racially and ethnically, respondents were homogeneous. Of those indicating race and ethnicity, 94% were white, and 97% were not Hispanic or Latino. Gender, age, education, and certifications data, however, show some differences. For example, 57% of the men had a master's degree versus 33% of the women. For certifications, gender differences were pronounced only for certified internal auditors (CIAs): 55% of the women were CIAs versus 33% of the men—similar to percentages for having a master's degree reversed by gender.

Directors' Gender, Age, Education, and Certifications
There were 89 men and 55 women.
– 73% of men were 50 years old or older
– 51% of women were 50 years old or older
Bachelor's degrees did not differ materially by gender; advanced degrees did.
– 57% of the men and 33% of the women had a master's degree
– 6 men and 1 woman had a doctoral degree
Ninety-two percent of respondents had at least one certification.
– 68% were certified public accountants
– 41% were certified internal auditors: 55% of women and 33% of men
– 20% were certified fraud examiners
– 16% were certified information systems auditors

Directors' Experience

Internal auditing experience was considerable. About half the respondents had over 10 years of expertise at their current institution. In addition, almost 90% had at least two years' experience outside of higher education and well over half had over five—primarily in public accounting, commercial enterprise, and government. Such respondents might know internal auditing and their institutions well and be able to make credible business comparisons. Women had somewhat less experience in all areas than men did.

Directors' Experience
Experience in internal auditing was considerable.
– In total: 75% had over 10 years, and 43% had over 20
– In higher education: 58% had over 10 years, and 25% had over 20
– At current institution: 48% had over 10 years, and 17% had over 20
Experience outside of higher education was appreciable and varied.
– 89% had at least two years; 56%, over five years; and 32%, over 10 years
– 44% in public accounting, 43% in commercial enterprise, and 36% in government

Institutions

One hundred four of the respondents' institutions (72%) were public, and 40 (28%), private. A similar percentage of each type had a medical school: 45% and 41%, respectively. Universities that had medical schools or were public tended to have higher enrollments, research funding, and total funding.

POSSIBLE INFLUENCING FACTORS

Older Men, CIAs, or Those at Institutions with a Medical School

Statistical tests using subsets of respondents identified factors possibly influencing views of culture and measuring achievement. Tests showed that the relationship between views of culture and measuring achievement was statistically significant with large effect size or strength for the 65 men who were at least 50 years old (older men) and for the 59 respondents who were CIAs. Such was true also for the 61 respondents at institutions with a medical school and the 57 at institutions with federal research funding over $100 million and a medical school.

Views of Both Culture and Measuring Achievement

Older men were more likely and CIAs less likely than respondents as a whole to view both culture and measuring achievement businesslike: percentages were 48% and 32% versus 38%. Also, CIAs and those at institutions with a medical school or with federal research funding over $100 million and a medical school were more likely than respondents generally to view both distinct: 41%, 38%, and 38% versus 30%. Also, older men were less likely than respondents as a whole to view culture distinct and measuring achievement businesslike: 17% versus 26%.

Views of Culture and Measuring Achievement		
Both businesslike		
Older men	**All**	**CIAs**
48%	38%	32%
Both distinct		
CIAs	**Had medical school or had over $100M in federal research and a medical school**	**All**
41%	38%	30%
Culture distinct/measuring achievement businesslike		
All		**Older men**
26%		17%

Views of Culture

Older men were more likely and CIAs less likely than respondents overall to view culture businesslike: 55% and 34% versus 44%. Male and female CIAs were less likely than respondents of their gender generally to view culture businesslike: 45% versus 51% and 23% versus 33%.

Viewed Culture Businesslike			
Older men	**All**		**CIAs**
55%	44%		34%
CIA effect?			
All males	**Male CIAs**	**All females**	**Female CIAs**
51%	45%	33%	23%

Views of Measuring Achievement

Respondents who were CIAs or at institutions with a medical school were less likely than directors as a whole to view measuring achievement businesslike: 58% and 59% versus 65%.

Viewed Measuring Achievement Businesslike		
All	**Had medical school**	**CIAs**
65%	59%	58%

Speculation about the Possible Influencing Factors

I speculate that older men, whose age and gender are comparable to those of many university board members from the business world, might be more likely to adopt, carry over, or value a business perspective. With internal auditing's origins in business, traditionalism might play a role too. Traditionalism does not imply outmodedness. After all, tradition imbues both the academy and culture itself in positive ways.

I speculate further that internal audit directors who were CIAs might have been more conscious of the Institute of Internal Auditors (IIA) Code of Ethics. The Code's principle of objectivity requires internal auditors to assess "all the relevant circumstances," and distinctness of culture and measuring achievement could have been considered apparent and pertinent. As for the medical school influence, perhaps activities such as educating physicians and providing community health services contribute to a sense of distinctness.

RANKINGS OF AUDITOR ATTRIBUTES, TYPES OF WORK, AND SUBJECT AREAS

Internal Auditing Factors

Respondents were also asked to rank the importance of five internal auditor attributes, five types of internal auditing work, and five subject areas of work at their respective institutions.

Internal Auditor Attributes

Skills in human relations and in oral and written communication were ranked the most important internal auditor attribute by 39% of respondents; awareness of higher education culture and missions, by 27%; and expertise in management and business subjects, by 20%. Expertise in accounting was ranked highest by 14%, and expertise in information technology (IT), by no one. The five attributes were ranked first or second in importance in the same order with these percentages: 79%, 50%, 45%, 22%, and 4%.

Internal Auditor Attributes	Ranked	
	1	1 or 2
Skills in human relations and communication	39%	79%
Awareness of higher education culture & missions	27%	50%
Expertise in management and business subjects	20%	45%
Expertise in accounting	14%	22%
Expertise in information technology (IT)	–	4%

Types of Internal Auditing Work

Operational audits were ranked the most important type of internal auditing work by 59% of respondents, and compliance audits, by 23%. Investigations were ranked highest by 10%; financial audits, by 7%; and IT audits, by 1%. The five types of work were ranked first or second in importance in the same order with these percentages: 77%, 64%, 25%, 18%, and 16%.

Types of Internal Auditing Work	Ranked	
	1	1 or 2
Operational audits	59%	77%
Compliance audits	23%	64%
Investigations	10%	25%
Financial audits	7%	18%
IT audits	1%	16%

Subject Areas of Internal Auditing Work

Finance and administration were ranked the most important subject area of internal auditing work by 66% of respondents, and sponsored research, by 22%. Academic operations were ranked highest by 8%; athletics, by 3%; and enrollment services, by 1%. The five subject areas were ranked first or second in importance in the same order with these percentages: 88%, 70%, 21%, 11%, and 10%.

Subject Areas of Internal Auditing Work	Ranked	
	1	1 or 2
Finance and administration	66%	88%
Sponsored research	22%	70%
Academic operations	8%	21%
Athletics	3%	11%
Enrollment services	1%	10%

VIEWS OF APPROPRIATENESS OF OPERATIONAL AUDITS IN MISSION AREAS

The internal audit directors were also asked whether they "strongly agreed," "mildly agreed," "mildly disagreed," or "strongly disagreed" that operational audits addressing accomplishment of missions and goals in research, teaching, and public service, respectively, were appropriate. About 75% agreed (strongly or mildly) that operational audits of research missions and goals were appropriate. Approximately 60% agreed, most of them mildly, that such audits of teaching and public service missions and goals were appropriate.

Are Mission Area Operational Audits Appropriate?					
Mission area	**Strongly agree**	**+**	**Mildly agree**	**=**	**Agree**
Research	41%		34%		75%
Teaching	17%		43%		60%
Public service	19%		42%		61%

RELATIONSHIPS WITH CULTURE AND MEASUREMENT ACHIEVEMENT VIEWS

Further testing found statistically significant relationships between (1) views of culture and rankings of internal auditing factors and (2) views of measuring achievement and agreement/ disagreement with the appropriateness of operational audits that address the accomplishment of research, teaching, and public service missions and goals. All effect sizes, and thus the strengths of relationships, were small.

View of Culture and Ranking of Internal Auditor Attribute and of Type of Internal Auditing Work

Those viewing culture distinct were more likely than those viewing culture businesslike to rank awareness of higher education culture and missions the most important internal auditor attribute: 36% versus 15%. Directors viewing culture businesslike were more likely than those viewing it distinct to rank operational audits first or second: 86% versus 69%.

View of Culture and Ranking of Internal Auditor Attribute	
Culture view	**Percentage that ranked awareness of higher education culture and missions the most important auditor attribute**
Businesslike	15%
Distinct	36%
View of Culture and Ranking of Type of Internal Auditing Work	
Culture view	**Percentage that ranked operational audits the first or second most important type of internal auditing work**
Businesslike	86%
Distinct	69%

Views of Measuring Achievement and of Appropriateness of Mission Area Operational Audits

Respondents who viewed measuring achievement businesslike were more likely than those who viewed it distinct to agree (strongly or mildly) that operational audits of research missions and goals were appropriate: 80% versus 64%. Respondents who viewed measuring achievement businesslike were also more likely than those who viewed it distinct to agree that operational audits of teaching missions and goals were appropriate: 68% versus 45%. The same was true for operational audits of public service missions and goals: 69% versus 45%. Conversely then, the majority, 55%, of those viewing measuring achievement distinct considered operational audits of teaching and public service missions and goals inappropriate.

View of Measuring Achievement and Percentage That Agreed Mission Area Operational Audits Were Appropriate

Mission area	Measuring achievement view	
	Businesslike	Distinct
Research	80%	64%
Teaching	68%	45%
Public service	69%	45%

For teaching and public service, strength of views data showed the possible influence that the view of measuring achievement had on the perceived appropriateness of mission-area operational audits. Of those viewing measuring achievement businesslike, 20% strongly agreed that operational audits of teaching were appropriate while of those viewing it distinct, only 12% did. For public service, comparable percentages were 24% and 10%. Moreover, of those viewing measuring achievement distinct, 25% strongly disagreed that operational audits of teaching were appropriate, while of those viewing it businesslike, only 9% did. For public service, comparable percentages were 18% and 8%.

View of Measuring Achievement and Percentage That Strongly Agreed (SA) or Strongly Disagreed (SD) That Mission Area Operational Audits Were Appropriate

	Measuring achievement view			
	Businesslike		Distinct	
Mission area	SA	SD	SA	SD
Research	48%	8%	28%	10%
Teaching	20%	9%	12%	25%
Public service	24%	8%	10%	18%

OTHER RELATIONSHIPS INVOLVING INTERNAL AUDITING FACTORS

Statistically significant relationships between rankings of internal auditing factors and between characteristics of institutions and ranking of subject areas of internal auditing work were also found. For this part of the study, at least a medium effect size or strength was requisite.

Ranking of Attribute and Ranking of Type of Internal Auditing Work.

Only the ranking of one internal auditing factor was statistically related to the ranking of another with at least medium effect size. Such was the case for ranking skills in human relations and in oral and written communication first and ranking operational audits first or second. Respondents who ranked skills in human relations and in oral and written communication first were more likely than those that did not to rank operational audits first or second: 93% versus 66%.

Ranking of Internal Auditor Attribute and Ranking of Type of Internal Auditing Work

Skills in human relations and in oral and written communication	Percentage that ranked operational audits the first or second most important type of internal auditing work
Ranked them the most important auditor attribute	93%
Did not rank them the most important auditor attribute	66%

Institutional Characteristics and Ranking of Subject Area of Internal Auditing Work

Another relationship with medium effect size involved respondents who were at institutions with over $100 million in federal research funding. They were more likely than those at institutions with $100 million or less in such funding to rank sponsored research as the most important, or the first or second most important, subject area of internal auditing work: 31% and 85% versus 12% and 56%. Similarly, again with medium effect, respondents who were at institutions with $100 million or less in federal research funding and no medical school were less likely than those not at such institutions to rank sponsored research first or second: 53% versus 81%. Of course, respondents at institutions with higher research funding, might have been more likely to have the substantial research enterprises that made sponsored research an area of consequential risk.

Institutional Characteristics and Ranking of Subject Area of Internal Auditing Work

Institutional characteristics	Percentage that ranked sponsored research the first or the first or second most important subject area of auditing work	
	Ranked it first	Ranked it first or second
Had > $100 million in federal research funding	31%	85%
Had ≤ $100 million in federal research funding	12%	56%
Had > $100 million in federal research funding or a medical school	*	81%
Had ≤ $100 million in federal research funding and no medical school	*	53%

*Relationship not statistically significant

SUMMARY AND CONCLUSION – ANSWERS IN THE QUESTIONS

Overarching Research Question

My overarching research question was whether internal audit directors' views about culture and measuring achievement differences between their respective institution and a business were related to how they viewed the priorities and uses of internal auditing at their institutions, including its use in mission areas.

How respondents viewed university culture was found to be related to the importance they attached to (a) internal auditors' awareness of higher education culture and missions and (b) operational audits. How respondents viewed measuring achievement was found to be related to how they viewed the appropriateness of operational audits in research, teaching, and public service.

The relationship found between being a CIA and one's views of culture and measuring achievement appears worthy of further investigation.

The CIA Relationships

The relationship found between being a CIA and one's views of culture and measuring achievement appears worthy of further investigation. In his study, Johnson found that 23% of internal auditors at public institutions and 36% at private institutions were CIAs.[4] My study of internal audit directors found comparable percentages by type of institution to be 39% and 48%, increases not unexpected after two decades. However, none of Fischer and Montondon's 209 study respondents reported holding the CIA designation.[5]

Viewing Culture Distinct May Put a Priority on Auditors' Awareness of Culture and Missions

Respondents with a distinct culture view were more likely than those with a businesslike culture view to have ranked awareness of higher education culture and missions the most important internal auditor attribute. More than a third of directors with a distinct culture view considered this attribute more important than know-how in accounting, IT, management and business, and human relations and communication. No attribute was ranked the most important more often by respondents with a distinct culture view. Yet, only about one-seventh of directors with a businesslike culture view ranked such awareness first. Of course, respondents who viewed institution culture businesslike might have thought such culture so inbred in internal auditors that awareness of it was of little importance.

Viewing Culture Businesslike May Put a Priority on Operational Audits

Directors holding a businesslike culture view tended to consider operational audits more important than did those holding a distinct culture view. Might then the former perform more such audits?

Viewing Measuring Achievement Businesslike May Favor Mission Area Operational Audits

Respondents with a businesslike measuring achievement view were more likely than those with a distinct measuring achievement view to consider operational audits in research, teaching, and public service mission areas appropriate. The majority of those who viewed measuring achievement distinct considered such audits of teaching and public service inappropriate and the percentages strongly disagreeing that they were appropriate were more than twice as large as those of respondents who viewed measuring achievement businesslike. Perhaps the former were implying that internal auditors cannot contribute in these areas. Are there then limits to what internal auditing should address, or where it belongs, at an institution of higher education?

Operational Auditing and Skills

Recall that respondents who ranked skills in human relations and in oral and written communication most important were more likely to have ranked operational audits first or second in importance. Operational audits tend to include and go well beyond financial principles, technology matters, and compliance concerns in helping to improve operations, so relating and communicating with others might have been viewed as vital.

These results are consistent with Azad and Skekel's study. Their respondents considered the human relations attribute of more than above average importance in encouraging management to devise solutions to deficiencies, one of only three factors, among 17, to be considered of that high importance within the context of operational auditing success.[6]

Are strong human relations and communication skills essential for internal auditors who assess classroom (teaching) and community (public service) missions? Over half of Azad's (1994) respondents reported having performed academic operational audits. He emphasized that academic functions had relevant and assessable elements for such reviews.[7]

Is the culture or are the ways of measuring achievement at your institution businesslike or distinct?

Questions and Answers

Is the culture or are the ways of measuring achievement at your institution businesslike or distinct? No matter the answers, the answers might matter. One answer might even be, "We need better questions." After all, in our profession and in our institutions' classrooms and laboratories, better questions lead to better understanding. ■

---

[1]Benjamin S. Roth, *Academic Culture, Business Culture, and Measuring Achievement Differences: Internal Auditing Views* (2012). *Educational Policy Studies Dissertations*. Paper 93. http://digitalarchive.gsu.edu/eps_diss/93.

[2]http://www.acua.org/ACUA_Resources/documents/ACUACandUJournalSpr13-FinalWeb.pdf

[3]Statistical methodology is described in the dissertation. Link to dissertation is in footnote 1.

[4]Gary G. Johnson, "Internal Auditing in Higher Education Institutions," *Internal Auditing*, 8 (Fall 1992): 53-58.

[5]Mary Fischer and Lucille Montondon, "Qualifications, Diversity and Workplace Practices: An Investigation of Higher Education Internal Audit Departments," *Journal of Public Budgeting, Accounting & Financial Management*, 17 (Winter 2005), 488-521.

[6]Ali N. Azad and Ted D. Skekel, "Personal Attributes and Effective Operational Auditing: Perceptions of College and University Internal Auditors," *Association of Government Accountants Journal*, 39 (Issue 3, 1990): 55-61.

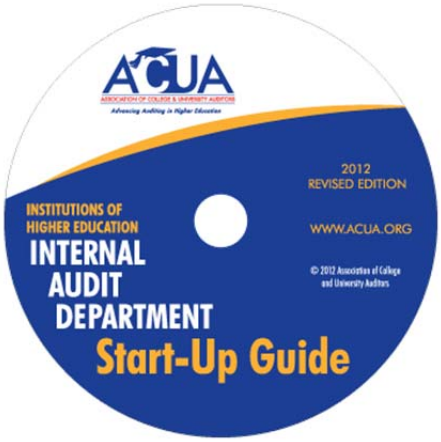
[7]Ali N. Azad, "Operational Auditing in US Colleges and Universities," *Managerial Auditing Journal*, 9 (Issue 2, 1994): 12-19.

ASSOCIATION OF COLLEGE & UNIVERSITY AUDITORS

INSTITUTIONS OF HIGHER EDUCATION

INTERNAL AUDIT DEPARTMENT

START-UP GUIDE



The primary purpose of this guide is to serve as a reference tool, one of many you will likely use as you establish an audit function that best fits the needs and resources of your organization. The information and examples have been collected from very successful audit shops and truly represent many of the best practices in higher education internal audit. They may or may not fit your needs, but they will all provide valuable guidance and ideas as you work to establish your new audit department.

Contents of this guide include:

- **Establishing the Authority of the Department with sample charters and policies**
- **Getting the Department Operational, with concrete advice on risk assessments, annual planning, quality assurance, fraud investigations, and marketing the new department**
- **Reporting to all constituencies, including examples of reports used by ACUA members**
- **List of resources and key terms**
- **And so much more!**

Please contact the ACUA Executive Office at acua-info@goAMP.com, call 913.895.4620 or visit the ACUA Store on ACUA's website www.acua.org for more information.

Are You Auditing Your Student Health Center? If Not, Why Not?

By LaDonna Flynn, CPA, CIA, CCSA

As you read the above article title, you are probably wondering, why should the university's auditor be worried about the student health center? Well, just because the student health center resides on your campus does not mean it is exempt from the various associated risks with the health care industry. By the time you finish reading this article, I hope you will understand the reasons for adding your student health center to your audit plan and have a guideline for your audit program.

It is important to consider the financial, operational and compliance risks facing a student health center.

It is important to consider the financial, operational and compliance risks facing a student health center.

- Financial risk: the risk that the financials are not accurate and do not aid in decision-making.
- Operational risk: the risk that processes do not run smoothly and help the organization meet their objectives.
- Compliance risk: the risk of non-compliance with laws and regulations.

Because the health care industry is one of the most highly regulated industries, the compliance risk associated with a student health center is high. The following section discusses the various risks associated with a student health center. Some of these risks can be categorized into all three types of risks.

An auditor should consider the following risks when evaluating whether to include a student health center in the annual audit plan or when developing a risk based audit program.

- **Health Insurance Portability and Accountability (HIPPA):** Is the student health center in compliance with the privacy standards (protection of personal health information) and the security standards (protection of electronic personal health information) of HIPPA?
- **Employee Safety:** Is the student health center in compliance with OSHA regulations surrounding a health clinic? Has the clinic protected its employees from blood borne pathogens from used needles? Does the health center have policies and procedures for infectious disease exposure?

Because the health care industry is one of the most highly regulated industries, the compliance risk associated with a student health center is high.

- **Malpractice:** Does the student health center have adequate malpractice insurance coverage? Who pays for the malpractice coverage, the provider or the university?
- **Patient Safety/Medication Errors:** Does the student health center have policies and procedures to prevent wrongful treatments being performed on a patient and/or the wrong medication being administered to a patient?
- **Informed Consent:** Does the student health center have the patient sign an informed consent? Informed consents are both an ethical obligation and a legal requirement spelling out in statute and case law in all 50 U.S. states.
- **Licensures:** Does the student health center have the correct licenses to practice in your state? Are the licenses current? Does your staff have current licenses to practice in your state and are the licenses current?

ABOUT THE AUTHOR

***LaDonna Flynn, CPA, CIA, CCSA**, serves as Internal Auditor at Pittsburg State University. LaDonna leads the internal audit department at PSU, which includes herself and one graduate assistant. At PSU, she serves on several committees including Data Classification Group, PCI Committee, Stakeholder Task Force, and Unclassified Senate. For the 2012-13 academic year, she served as PSU's IAEP Coordinator. Prior to PSU, she was an Audit Manager with CHAN Healthcare Auditors in Tacoma, Wash. and Tucson, Ariz.*

- **Patient Admitting & Registration (Eligibility):** Is the student health center only seeing patients who are eligible to be seen at the student health center? Is the student health center reviewing the patient's identification to ensure the patient is actually whom they say they are?
- **Billing/Charge Capture/Coding/Charge Master:** Is the student health center capturing charges correctly? Do the charges match the patient's medical records? Does the student health center have charge master policies and procedures? Are the charge master policies and procedures adequate?
- **Cash Activities:** How is the student health center collecting for charges? Is there adequate segregation of duties between who posts the charges and who collects the payment?
- **Managed Care:** Is the patient's insurance company being billed by the student health center? Is the insurance company paying the student health center correctly? Is the insurance company charging the students the correct insurance premiums?
- **Americans with Disabilities Act (ADA):** Does the student health center provide reasonable accommodations to patients with disabilities? How does the student health center handle patients who do not speak English?
- **Emergency Medical Treatment and Active Labor Act (EMTALA):** Is the student health center providing emergency care 24/7?
- **Health Care Fraud and Abuse:** According to the federal government, fraud and abuse is rampant in health care. Is there fraud and abuse occurring at your student health center?
- **Pharmacy:** Does the student health center have an on-site pharmacy? If yes, how are the medications controlled (ordering, receiving, dispensing)?
- **Laboratory:** Does the student health center have an on-site laboratory? If yes, is the equipment adequate and being maintained? Are the labs being performed supported with a signed physician order?
- **Radiology:** Does the student health center have an on-site x-ray? If yes, is the equipment adequate and being maintained? Are the x-rays being performed supported with a signed physician order?

The ACUA website has a risk dictionary, resource library, and list serve.

Based on the annual risk assessment, an audit of the student health center has been added to the plan. So, now what? As with any audit, it is time to start planning the audit. The first step for Pittsburg State University's (PSU's) internal audit department is to perform research on the subject of student health centers. Some valuable resources are the ACUA website and Google. The ACUA website has a Risk Dictionary, Resource Library, and the ACUA-L Listserv.

The next planning step for PSU's internal audit department is to perform interviews. To determine who to interview, a review of the university organization chart is helpful. At PSU, the potential interviewees included the president, vice president of campus life and activities, the director of operations at the Student Health Center, and the medical director at the Student Health Center. PSU's reason for interviewing the president and vice president is because internal audit reports to the president and the student health department reports to the vice president. The questions for the president and the vice president helped identify any areas of concern regarding the Student Health Center. The questions for the director of operations and the medical director included what services are they providing, how are fees charges/collected, what services do they charge for, and who is eligible for services, are the providers full-time or part-time under contract, and how do they maintain their medical documentation. The director of operations was also asked to provide copies of all policies and procedures, and departmental usage reports.

Based upon our review of the research, interview notes, policies and procedures, and departmental usage reports, it was determined that PSU's Student Health Center:

- Provided unlimited free office visits for enrolled students with charges for medications, x-rays, laboratory tests, and procedures.
- Provided outpatient medical/surgical services, physicals, women's/men's health services and had an on-site pharmacy, laboratory, and radiology department.
- Maintained the patient's medical and billing records in the Point and Click system.

- Have one part-time medical director, three nurse practitioners, three RNs, and one radiology technician.
- Have 7 exam rooms, 1 triage room, 1 procedure room, and 1 recovery room.
- Have 13,256 encounters in academic year 10-11 and 12,475 encounters in academic year 11-12. An encounter is the process of a patient coming in to see a provider. Each time a patient sees the provider it counts as an encounter. This is a standard benchmarking statistic maintained in health care.
- Have never been audited.
- Have moved to a new building in 2009.
- Have a new medical director in 2011.
- Have received a complaint from the prior medical director about their processes. The complaint said the student health center was seeing patients who were not eligible for services.
- Was not inspected by the State Department of Health. In Kansas, student health centers are exempt from inspections.
- Was to have a wide scope due to the complaint and at the request of the president.

Based on the above information, it was decided to focus the audit on the following processes eligibility, fee collection, charges, registration, cash activities, pharmacy controls, licenses, and informed consent.

- **Eligibility:** The Student Health Center had seen a patient that was not eligible for services, had any more ineligible patients been seen.
- **Fee collection:** At PSU a part-time student pays a specific amount per hour for fees and a full-time student pays a set fee. The fees go towards student health, parking, student union, athletics, etc. Was the Registrar's office billing and the Cashier's office collecting the correct amount of fees?
- **Charges:** Was the Student Health Center charging the correct amount based on what the provider documented in the medical records? Were the patients being charged for the medication being dispensed from the Pharmacy? Were the patients being charged for their labs and x-rays? If a patient could not pay for services, were holds being placed in the patient's university account?
- **Registration:** Was the Student Health Center checking for eligibility when the patient both made an appointment and came in for their scheduled appointment? Was the Student Health Center checking the patient's identification?
- **Cash Activities:** Was the Student Health Center's cash handling controls adequate?
- **Pharmacy:** Did the Student Health Center have adequate inventory controls, receiving, ordering, and dispensing?
- **Licenses:** Did all employees, who needed licenses, have current licenses and did the Student Health Center have all the necessary licenses?
- **Informed Consent:** Was the Student Health Center obtaining all the correct documentation at the patient's registration?

Based on the above focus and questions, the audit scope and objectives for the audit were developed. The scope would cover 2011 and 2012 fiscal years. The audit objectives were as follows:

- To determine whether the Bryant Student Health Center had adequate, suitably located facilities, adequate technology, and equipment to support its mission and goals efficiently and effectively.
- Determine that eligibility for services were appropriately determined prior to treatment and/or consultation. To determine existence, completeness, timeliness and accuracy of revenues collected and recorded.
- To test internal controls operating over the receiving, processing, banking and accounting for all cash collections at student health center.
- Determine that management consistently monitored and assessed the adequacy and patient satisfaction with services and facilities, provider performance, and the quality of patient care.
- To determine Student Health Center employees were qualified and compliant with licensing regulations and PSU's policies, including training and testing.
- To determine whether pharmacy operations at PSU's Bryant Student Health Center meet the needs of patients and were provided in accordance with professional and ethical standards.
- To determine whether there were adequate controls over the acquisition, storage, and issuance of medications.

- To determine whether the Student Health Center had established appropriate policies and procedures for responding to emergency situations.
- To test the Student Health Center's management of financial resources to determine the activities were in compliance with the mission of the Center and the University.

As part of the planning process, PSU's audit department identified the possible obstacles that could be faced during the audit. The scope of the audit was huge and would require a lot of time for a 1.5 person internal audit shop. The Student Health Center had said they would not let the internal audit department's graduate assistant perform any testing that involved her looking at patient records. The data in the Student Health Center's Point and Click system (PNC) was maintained differently than the data in PSU's financial system. The PNC system had the details and PSU's financial system had high-level summaries.

From the audit objectives, internal audit developed the related audit steps to test the audit objectives. The remainder of this article will focus on the detailed audit steps used for the audit at PSU Student Health Center (SHC).

I. Audit Objective: To determine whether Bryant Student Health Center has adequate, suitably located facilities, adequate technology, and equipment to support its mission and goals efficiently and effectively.

Audit Steps:

A. Collect evidence to assess the suitability of PSU facilities, technology, and equipment relative to the stated mission and goals. Consider at least the following factors:
   1. Adequate reception areas, toilets and telephones
   2. Suitable access and accommodations for patients with disabilities
   3. Adequate lighting, heating, and ventilation
   4. Cleanliness of facilities
   5. Confidentiality and privacy of services and records
   6. Testing and proper maintenance of equipment

B. Ascertain if the SHC has been evaluated and accredited by a nationally recognized, independent review agency.
   1. Review the most recent accreditation report and evaluate how management addressed noted recommendations.
   2. Verify that copies of accreditation reports are forwarded to the campus president and Associate Vice President for Campus Life & Auxiliary Services.
   3. Review and evaluate management's efforts to prepare for pending accreditation surveys.
   4. For non-accredited campuses or campuses with deferred or provisional accreditation, evaluate management's actions and follow-through to obtain full (three-year) accreditation.

II. Audit Objective: Determine whether eligibility for services is appropriately determined prior to treatment and/or consultation. To determine existence, completeness, timeliness and accuracy of revenues collected and recorded.

Audit Steps:

A. Ascertain whether student health center eligibility guidelines (e.g., services to regular continuing students, summer session students, etc.) are in accordance with guidelines.
   1. Interview the receptionist and/or other front office staff to verify how they determine patient eligibility prior to rendering services (consider students from other campuses in your testing).
   2. Observe students registering at the front office to determine if guidelines are being followed.

B. Using scheduling/treatment records, judgmentally select medical files for patients seen at the Student Health Center for the time period under audit. Test for the following:
   1. Verify that necessary forms (e.g., patient history, laboratory reports, x-ray results, etc.) as required by department policy and/or accreditation standards are in file and properly completed.
   2. Services fall within established guidelines
   3. The medical record is complete by the physician or nurse practitioner and matches the services the student received.
   4. The patient was properly billed for services rendered.
   5. The patient paid for and the receipts were deposited for the services rendered.

C. Compare the list of patients in the medical record file to the student file in register's using V-lookup for either student ID number or student Social Security numbers.

III. Audit Objective: To test internal controls operating over the receiving, processing, banking and accounting for all cash collections at the Student Health Center.

Audit Steps:

A. Document processes and controls for the following:
   1. Cash and check collections & deposits
   2. Credit card collections & deposits
   3. Ensure proper segregation of the following functions:
      - Collection of cash
      - Preparation of deposits
      - Recording transactions

B. Determine the procedures for closing the register and balancing the cash drawer and ensure that proper internal controls exist to safeguard cash collected.

C. Observe the balancing of the cash drawer to the register. Conclude as to whether internal controls are adequate. Review daily balancing documentation and ensure that the supervisor signs it.

D. Select a representative sample of collections days from the audit period to trace from initial receipt to deposits.

IV. Audit Objective: Determine whether management consistently monitors and assesses the adequacy and patient satisfaction with services and facilities, provider performance, and the quality of patient care.

Audit Step:

A. Review and evaluate the controls over patient suggestions and complaints.
   1. Select a random sample of patient suggestions and/or complaints and confirm appropriate handling and resolution. Ensure the patient was timely informed of the outcome and that all results are escalated to the SHC Director or his/her designee.
   2. Ascertain if patient complaints are considered in management's evaluation of provider staff performance, student health services, facilities, etc.

V. Audit Objective: To determine whether Student Health Center employees are qualified and compliant with licensing regulations and PSU policies, including training and testing.

Audit Steps:

A. Document the education and certification requirements of personnel employed in Student Health Center based on a review of position descriptions.

B. Verify that all of the employees required to maintain a current license have a current license.

C. Document staff participation in continuing professional education. Investigate and document any deficiencies related to professional standards.

VI. Audit Objective: To determine whether pharmacy operations at PSU Bryant Student Health Center meet the needs of patients and are provided in accordance with professional and ethical standards.

Audit Steps:

A. Review for evidence of current licensure by the state of Kansas. Note: Licenses must be renewed annually.

B. Observe the SHC Pharmacy for the following:
   1. The Pharmacy door is locked at all times.
   2. Only persons authorized are permitted access and only when a licensed pharmacist is present.
   3. Controlled substances are kept in a locked cabinet and only accessible to authorized personnel.
   4. Through observation, verify that activities are monitored.

C. Document the standards for the Pharmacy by the state.

VII. Audit Objective: To determine whether there are adequate controls over the acquisition, storage, and issuance of medications.

Audit Steps:

A. Obtain and review pharmacy policies and procedures.

B. Document where the various medications are stored.
   1. Drugs requiring refrigeration are monitored.
   2. Drugs requiring light protection are covered with amber plastic wrap.
   3. Verify that any medications not in their original packing are adequately identified and properly stored.

4. Verify that physician samples are properly received, stored and dispensed including notation in patient charts.

C. Discuss with RN how medications are ordered and received. Document what controls are in place to ensure:
   1. Adequate levels are ordered to prevent shortages and costly drop shipments.
   2. Medication received is accounted for by a person independent of the receipt function.
   3. A method exists for receiving vendor credit for shortages or drugs returned that were not ordered.

D. Observe the Medication Order Entry process from beginning to end and determine the following:
   1. The patient's profile is checked by the pharmacist.
   2. The doctor's orders are checked by the pharmacist entering the order into PNC for completeness and clarity.
   3. Check labels are verified against the doctor's order prior to the drug being dispensed.

E. Observe and document the process of distributing medicines to the patients/students.

F. Review and evaluate the SHC's inventory control procedures.
   1. Verify that the Pharmacy's inventory system records, reports, etc., are current and appropriately account for all medications (including over-the-counter and controlled substances), and supplies.
   2. Using the inventory records, perform a random inventory of medications, and a complete inventory of controlled substances, to the perpetual inventory records. While performing the inventory, sample drugs in stock to ensure there are no outdated, discontinued, or recalled drugs in stock.
   3. Ensure there is adequate segregation of duties between the persons who handle the Pharmacy inventories and those handling inventory records, sales billings, and recording of purchases.

G. Verify through observation and interview the process for disposing expired items (including controlled substances), and handling recalled drugs.

VIII. Audit Objective: To determine whether the Student Health Center has established appropriate policies and procedures for responding to emergency situations

Audit Step:

A. Obtain copies of policies and procedures for responding to emergency situations.
   1. Evaluate the sufficiency and consistency of policies and procedures. Investigate and document any deficiencies.
   2. Evaluate policies and procedures for access to personal health information in emergencies.

IX. Audit Objective: To test the Student Health Center's management of financial resources to determine the activities are in compliance with the mission of the Center and the University:

Audit Steps:

A. Obtain budget reports from the GUS and/or Administrative system that identifies the revenues and expenditures of the department's financial units.

B. For expenditures:
   1. Select a judgmental sample of expenditures made by the department during scope of the audit.
   2. Review for adherence to policy and any restrictions.
   3. Review for adequacy of documentation including business purpose, proper approvals, original receipts, etc.
   4. Evaluate results and expand testing if required.

C. For revenues:
   1. Select a judgmental sample of revenue transactions from the receipts during the scope of the audit.
   2. Trace to deposit in appropriate account.
   3. Review for timeliness of deposit.
   4. Evaluate results and expand testing if required. ■

Putting the "Enterprise" in Enterprise Risk Management

By Cheryl Lloyd, Carrie Frandsen, MBA, ARM, Emily Breed, Kimberly A. Newman and Erin Ann Thomas

With more than 190,000 employees, 33,000 lines of business, 10 campuses, 5 medical centers, 3 national laboratories, and oversight for the statewide 4-H program, the University of California (UC) has to be enterprising and resourceful in how it manages risk.

Risk management at UC used to be highly decentralized and traditional. In 2004, UC's Office of the President (UCOP) realized that risk management needed to be more strategic and have a systemwide orientation. This was a shift in attitude and orientation, not in the authority wielded by UCOP, as each campus has significant autonomy when making strategic and operational decisions. "Our role is to support the campuses in their risk management activities," says Carrie Frandsen, systemwide program manager for Enterprise Risk Management (ERM). "We can't tell them what to do; we have to persuade them that we have good ideas that will provide value to them."

The UC System began an ERM initiative as a natural progression after adopting the COSO (Committee of Sponsoring Organizations of the Treadway Commission) Internal Control – Integrated Framework in 1995 and learning of COSO's publication of the Enterprise Risk Management – Integrated Framework in 2004. The COSO frameworks, as opposed to more traditional views of internal controls and enterprise risk management, are particularly suited to a university setting due to their broad view of the organization: everyone has a role, starting with the Board of Regents and the Audit Committee. This broad organizational view focuses first on the environment and the messages sent by the organization leaders, referred to as the tone at the top.

This top-down energy has resulted in the implementation of more than 30 tools and systems, 46 dashboard reports, and over $196 million of savings from ERM initiatives in just three years. The latter results allowed for redirection of administrative costs to investments in the University's core missions of teaching, research, patient care and public service.

In keeping with our shared governance model, UC Risk Services provides infrastructure to increase efficiency, enhance performance and reduce cost of risk throughout the system, but ultimately the management of campus and medical-level risks depends on each location's on-site risk management engagement at every level. This is why the slogan of our systemwide ERM program is "Everyone is a Risk Manager." Equipped with the tools to succeed, we are working to support user adoption of new risk management systems, processes and behaviors in order to reach the peak of administrative excellence.

PROVIDING ACCESS

We created the My Managed Risk (MMR) Portal as a central entry point, providing individuals access to UC's sophisticated suite of risk management tools from one location through a single sign-on. Each portal user's view is customized to allow access only to the user's authorized ERM applications. Available resources span levels of technological literacy from Excel risk assessment tools to complex planning, budgeting and forecasting tools. Our ERM Service Desk, located at UC Davis, provides support for our entire suite of online tools,

Available resources span levels of technological literacy from Excel risk assessment tools to complex planning, budgeting and forecasting tools.

ABOUT THE AUTHORS

Cheryl Lloyd *(left) is the Chief Risk Officer for the University of California, Office of the President, and oversees the University's extensive ERM program and Working Smarter initiatives. Major focuses include reducing the cost of risk, improving claims management, and overseeing business continuity planning. Before serving as CRO, Cheryl served as the Director of Liability and Property Programs. She has also worked at Chubb Insurance and Core-Mark International.*

Carrie Frandsen, MBA, ARM, *(right) has five years' experience managing higher education ERM programs. She is the ERM Program Manager with UCOP's Office of Risk Services. Prior to joining UCOP, Carrie was the Manager, Enterprise Risk Services with UC Santa Barbara, having responsibility for the ERM, Emergency Management, and Continuity Planning programs.*

including responding to requests for access, providing answers to user questions and troubleshooting issues.

The Enterprise Risk Management Information System (ERMIS), our data repository and network of dashboards, provides 157 key risk and performance indicators to support tasks ranging from monthly reporting to advanced data analysis. The Safety Index, a pilot dashboard released in 2009, displays comparison data across UC locations for workers' compensation and general liability events; the cumulative normalized percentages are presented with other measures to each campus's vice chancellor in the Quarterly Enterprise Risk Report, along with annually updated maturity model measures of ERM adoption. Since 2010, the CFO Actionable Information for Managers (AIM) report has provided key metrics from each location in 18 reports showing campuses side by side on various measures. As well as helping campus staffs target problem areas, the visibility dashboards have served as a powerful impetus for each campus and medical center to strive for greater efficiency and to seek out best practices.

One way of encouraging risk managers to champion new risk management solutions is by creating champions

DEVELOPING EXPERTISE

One way of encouraging risk managers to champion new risk management solutions is by creating champions. The purpose of the Centers of Excellence (CoEs) is just that. The UC has designated staff members from the campuses and medical centers to lead efforts to gather subject matter experts, research and study materials on various topics, including behavioral intervention, ergonomics, laboratory safety and technology. Now 17 CoEs hosted at different sites provide educational opportunities and develop standards and success criteria for their areas of expertise. The CoEs are tasked with systemwide leadership responsibilities, including providing assistance to other campuses.

After a devastating fall injury in 2008 in the theatre arts program and a costly lawsuit, UC Santa Cruz began to more seriously examine risks in this area. In 2012, the Theater Arts CoE was formed. Brent Cooley spent his first six months on the job visiting UC campuses to evaluate the status quo. From his contacts, he started a listserv with 65 subscribers, where he regularly provides health and safety information. Cooley is in the process of developing the UC Theater Arts Safety Manual, which will help individuals identify safe work procedures for specific work duties. In August 2013, Cooley coordinated a systemwide theater safety meeting at which Disney presented safety tips and vendors showcased safety products.

ENCOURAGING INNOVATION FROM THE BOTTOM UP

The Be Smart About Safety (BSAS) Program is another mechanism by which we provide staff members an opportunity to implement good ideas. Individuals submit proposals for loss prevention initiatives to reduce workers' compensation costs. Approved proposals receive funding from UCOP. In 2010, ERMIS reports indicated a high rate of claims from slip and fall injuries at UCLA. In response, UCLA risk managers requested support from UCOP for a nonslip-shoe program. Initially the program focused on food service workers. As the data began to show that the program was significantly reducing injuries, UC expanded it to other staff members, ultimately reducing slip and fall accidents by 50% systemwide. UC's actuaries have calculated that the BSAS program has provided an average return on investment of 2:1, and several BSAS prevention efforts have experienced a return as high as 5:1.

SHARING BEST PRACTICES

In 2005, we held our first Risk Summit, where 143 individuals involved in university risk management were challenged to strategically reduce the cost of risk by 15 percent in two years, focusing on areas such as ergonomics, foreign travel, loss prevention and workers' compensation benchmarking. Each year since, the conference has grown and included a wider range of attendees. Participants convene at Risk Summit each year to share best practices, network and learn about the new systems supported through Risk Services. Attendees come from a range of disciplines throughout the university community including continuity planners, controllers,

ABOUT THE AUTHORS

Emily Breed *(left) is an analyst with UCOP's Office of Risk Services. During her eight years with UC, she has worked on a range of enterprise risk management projects and initiatives. Before joining UC, she worked as a research associate at the Kaiser Permanente Division of Research.*

Kimberly A. Newman*, (right) IBM Senior Managing Consultant, has ten years of technical, financial, and project management experience in higher education, and Scrum Master and Project Management Institutes certifications. Prior to joining IBM, Ms. Newman served as Senior PM and Coordinator for the UC Office of the President. Currently, she serves as the PM for the UC Enterprise Risk Management Information System (ERMIS).*

Erin Ann Thomas*, IBM Senior Consultant, has four years of consulting experience and nine years of teaching experience. She currently supports the UC Enterprise Risk Management Information System (ERMIS) implementation. In addition to her consulting activities, Ms. Thomas is an award winning nonfiction author, and has published a number of academic and creative texts.*

counseling professionals, directors of recreational sports, EH&S (Environment, Health & Safety), emergency managers, fire marshals, human resources/disability managers, the Office of General Counsel, police chiefs, risk managers, student affairs, student health services and wellness. The conference has proved to be an excellent vehicle for raising risk management consciousness, increasing use of the new systems and improving overall staff effectiveness. More than 1,200 participants attended the 2013 conference. Session titles included topics as diverse as "Computer-Administered ADHD Screenings for Improved Risk Management" and "Farm to Fork: Foods Risk Management." Brent Cooley presented the session "Safety in Theatre Arts," and Barclay W. Ogden shared "PRISM in ERM in Practice: A Case Study on Protecting Library Assets." In total, 40 professionals showcased information about their particular areas of expertise.

The conference has proved to be an excellent vehicle for raising risk management consciousness, increasing use of the new systems and improving overall staff effectiveness.

BUILDING ON THE "POWER OF 10"

Of course, each UC location is unique, as campus risks differ from medical center risks, and risks vary across campuses due to differences in size, student population, location, academic focus, and more. At the same time, our locations have many common risks and requirements. Rather than try to centrally assess needs and create solutions at UCOP, we find it is more effective to support the creative efforts taking place throughout the system.

UC Davis Information Technology Services is a UC ERM CoE for Technology. As part of its current work, this UC Davis organization is developing a suite of EH&S online applications that aid researchers, their staffs and EH&S personnel in managing risks inherent to a laboratory setting. These applications include chemical inventory tracking, developing laboratory standard operating procedures, tracking laboratory safety processes, and tracking the disposal of hazardous waste.

Development of these applications includes gathering feedback from early adopters, which facilitates valuable feature upgrades and enhancements that make applications suitable to wider audiences. Each campus, of course, has specific needs and requirements for its users. Bringing individual requests to the development teams and the subject matter experts for each project ensures that products are created with a depth that will accommodate the majority of users on any given campus.

One of the more recently developed applications is the Laboratory Hazard Assessment Tool (LHAT). This application allows Principal Investigators to identify the hazards in their labs and assign appropriate personal protective equipment (PPE) to their lab workers based on their specific research activities. The application provides a hazard assessment, determines what PPE should be used, directs users to a safety training module, and then produces a printable voucher redeemable for appropriate PPE.

These applications are tied together with middleware, which stores information about people, locations and facilities that are common to the above EH&S applications. Principal Investigators and their staffs benefit as the middleware provides a user-friendly interface, and EH&S gains better data to manage compliance with state and federal regulations.

Through these strategies and others, we endeavor to make "Everyone is a Risk Manager" not just a slogan, but a reality.

EVERYONE IS A RISK MANAGER

Through these strategies and others, we endeavor to make "Everyone is a Risk Manager" not just a slogan, but a reality. Enterprise risk management requires addressing risk at all levels of an organization and ensuring that all members understand why and how their efforts matter, analogous to a jigsaw puzzle in which one missing piece leaves a gap or to a stone arch which will collapse if one stone is removed. By spreading the message that "Everyone is a Risk Manager" and by giving members of the University community the knowledge and tools they need to improve efficiency, create value and increase safety, we are raising UC's administrative and operational efficacy while continuing to focus on our core missions of teaching, research, patient care and public service. ■

TeamMate®

Audit Management System

More Accessible than Ever for ACUA Members

We're excited to announce that TeamMate has partnered with ACUA to provide exclusive benefits to ACUA members. The entire ACUA Risk Dictionary is now available within TeamMate, and ACUA members can now leverage the buying power of its entire membership to make TeamMate more accessible than ever.

Learn more at **www.TeamMateSolutions.com/ACUA**

Wolters Kluwer

Audit, Risk & Compliance

Managing Information Technology Compliance Risk

By Carlos S. Lobato, CIA, CISA, CISSP

As colleges and universities continue to embrace technology to meet their strategic objectives, the need to navigate a complex information technology (IT) regulatory landscape must not be overlooked. Clearly, IT laws and regulations have important intentions and purposes, such as safeguarding users' data. But ensuring compliance with so many and often overlapping state and federal regulations can become a daunting task. In 2012, New Mexico State University (NMSU) took the first step toward achieving this goal when it created its IT Compliance Function and hired an IT compliance officer.

As colleges and universities continue to embrace technology to meet their strategic objectives, the need to navigate a complex information technology (IT) regulatory landscape must not be overlooked.

The IT compliance officer is charged with performing university-wide IT risk assessments for information security and compliance. Additionally, the IT compliance officer develops, implements and monitors IT policies and procedures. The IT compliance officer works collaboratively with internal audit and IT security, with a common goal of reducing the risks that threaten the availability, confidentiality and integrity of the University's technologies and data.

Many colleges and universities give the role of managing IT compliance to the Chief Information Security Officer (CISO). And there were discussions at NMSU about who should lead this effort. But because the CISO role had not been created, it was determined that an IT compliance officer would provide a solid foundation for NMSU to begin enhancing its information security maturity level by focusing on compliance. Additionally, prior to the hiring of the IT compliance officer, previous IT auditors did not feel comfortable guiding staff in the proper remediation steps. The IT compliance officer would not have these perceived audit independence issues.

To be successful, an IT compliance officer should have a combination of technical, audit, strategic and communication skills. The NMSU publicized job description required a minimum of eight years of experience in IT audit or other technical work with professional credentialing such as Certified Information Systems Auditor, Certified Information Systems Security Professional or Global Information Assurance Certification being desirable. The IT compliance officer should be able to see the big picture and be savvy about conducting risk assessments that uncover high risks areas. The IT compliance officer should be able to speak with top-level management in a manner that avoids technical jargon about the biggest challenges. Additionally, the work of an IT compliance officer should be documented in order to properly demonstrate compliance.

The IT compliance officer should be able to speak with top-level management in a manner that avoids technical jargon about the biggest challenges.

BENEFITS

The following represent some of the benefits to date of having an IT compliance function at NMSU:

- Formal identification, comprehension and communication to the University community of federal, state and industry regulations applicable to the IT activities of NMSU.
- University-wide IT risk assessments formally conducted and documented, resulting in the identification of high risk areas and the creation of a five-year IT compliance working plan approved by the Chief Information Officer.

ABOUT THE AUTHOR

Carlos S. Lobato, CIA, CISA, CISSP *is New Mexico State University's IT compliance officer. He is responsible for ensuring IT activities comply with applicable regulatory requirements. Carlos has extensive private, banking, local government and higher education auditing experience and holds both auditing and technical IT certifications.*

- The creation in 2012 by the NMSU Information and Communication Technologies Department (ICT) of an IT Compliance Framework for Institutions of Higher Education, presented at various conferences, including one sponsored by the Association of College and University Auditors. Feedback has been positive.
- Work on proactive activities, such as IT governance, data governance and IT policies, aimed at benefitting NMSU holistically. Emphasis is on preventing data breaches.
- Work and collaboration with the University's IT auditor and outside auditors.
- Continual work on training and awareness programs as they relate to information security, regulatory compliance and the prevention of data breaches for regulated data and Personally Identifiable Information (PII).

IDENTIFICATION OF LAWS AND REGULATIONS

The first step for the IT compliance function was to compile a list of all the federal and state laws and industry regulations that apply to the IT activities of the University. There are laws and regulations that apply directly and some that apply indirectly to the IT activities of a college or university. Ensuring compliance with all applicable laws necessitates a risk-based approach. The following data privacy laws and regulations were identified as directly relating to the IT activities of NMSU:

- FERPA is the Family Educational Rights and Privacy Act of 1974, which requires control over the disclosure of student information.
- HIPAA is the Health Insurance Portability and Accountability Act of 1996, which requires control over the disclosure of medical information.
- GLBA is the Gramm-Leach-Bliley Act of 1999, which requires control over the disclosure of nonpublic information.
- RFR is the (Identity Theft) Red Flags Rule provision of the Fair and Accurate Credit Transactions Act of 2003, which requires control over the disclosure of Personally Identifiable Information.
- FISMA is the Federal Information Security Management Act of 2002, which sets forth information security requirements that federal agencies and any other parties collaborating with such agencies (grantees) must follow in an effort to effectively safeguard IT systems and the data they contain.
- PCI DSS is the Payment Card Industry Data Security Standards, which require the proper protection and safe handling of cardholder information.

There are other laws and regulations that indirectly apply to the IT activities of a university, such as copyright laws and the Communications Assistance for Law Enforcement Act. However, the preceding data privacy laws and regulations directly apply to IT activities and require the implementation of comprehensive information security controls to ensure data security, privacy and compliance.

An IT compliance function has an abundance of opportunity to provide value. Data privacy laws and regulations are very complex and may require in-depth review, analysis and discussions with many institutional stakeholders, such as legal counsel and audit, to properly assure, document and demonstrate compliance. Simply identifying and communicating to the institutional community what laws and regulations apply to the IT activities of the institution is crucial to meeting compliance requirements. At NMSU, a website for IT compliance (http://compliance.ict.nmsu.edu/) was created that includes a list of laws and regulations.

Regulatory compliance is complex, and sometimes management may be under the impression that they are compliant when they are not.

Regulatory compliance is complex, and sometimes management may be under the impression that they are compliant when they are not. Compliance requires formal documentation, and all of the above data privacy laws and regulations have checklists or audit programs to document and ensure compliance. For example, the U.S. Department of Education created the Privacy Technical Assistance Center (PTAC) to help guide colleges and universities in implementing technical security controls to protect data. The PTAC has created security checklists covering various subjects, including data governance, data security, data breaches, etc., to help assure compliance with FERPA. The U.S. Department of Health and Human Services has developed an audit program, which should be used by covered agencies to ensure compliance with HIPAA. These resources were brought to light by the IT compliance officer. Also eye-opening was that

Taking a risk-based approach to compliance has never been more important.

each regulation requires an ongoing program. Further, all of the above laws and regulations require establishment of clear institution-wide information security responsibility, creation of a formal written risk-based information security program, policies and procedures, and continual monitoring and training.

IT RISK ASSESSMENTS

Taking a risk-based approach to compliance has never been more important. After identifying the applicable laws and regulations and learning about their requirements, the institution should make a list of its risks. An IT compliance function, if leading the IT risk assessment, should ask management to rate those risks as high, medium or low and should establish an IT compliance working plan based on the risk appetite of the institution. Conducting a formal IT risk assessment and creating a working plan will help ensure alignment with the overall objectives of the institution and ensure proper mitigation and formal acceptance of risks.

At NMSU in 2012, the IT risk assessment identified the lack of formal IT policies and procedures as its number one risk, network access and security concerns as risk number two, and protection of sensitive and confidential data as risk number three. To address and mitigate those risks, NMSU outsourced a comprehensive network penetration test and vulnerability assessment to an external company that specializes in such activities. The IT compliance officer led the effort. Additionally, NMSU is in the process of updating and creating new policies as identified by an internal IT policy gap analysis. As of this writing, the NMSU Office of Audit Services has conducted follow-up audit work in these areas, finding significant improvement but with work still needed in some areas. The responsibility to ensure risks are properly addressed belongs to management. However, the IT compliance officer should ensure the IT Compliance Function working plan addresses the highest risks and should promptly communicate noncompliance risks.

IT COMPLIANCE FRAMEWORK

After identifying applicable laws and regulations and conducting an IT risk assessment, in an attempt to avoid overlapping effort, the NMSU IT Compliance Function created a visual roadmap for management. This roadmap showed how to meet regulatory compliance. This roadmap facilitated NMSU ICT's creation of its university-wide IT compliance framework, mentioned earlier, to ensure compliance at a high level with all of the previously identified federal and industry laws and regulations (FERPA, HIPAA, GLBA, RFR, FISMA and PCI). At NMSU, this framework is guiding our efforts to become fully compliant with regulatory requirements and to enhance our overall information security. NMSU is currently assessing and revamping university-wide PCI, Red Flags Rule, HIPAA, GLBA, FISMA and FERPA programs. Some programs will require outside expertise. For example, a PCI assessment will require the skills of a Qualified Security Assessor (QSA) because NMSU does not have a QSA.

The message and attitude of an IT compliance function should always be that proactive activities and measures should be put in place instead of waiting for a data breach to happen.

PROACTIVE IT COMPLIANCE ACTIVITIES

An IT compliance function can help identify areas where improvement is needed, especially areas that may have broad applicability within the institution. At NMSU, the IT Compliance Function has identified IT governance and data governance as areas needing improvement. As of this writing, NMSU is assessing its current IT and data governance practices, which will likely result in their becoming more formal. Institution-wide IT policies would be another area in which an IT compliance function can provide value, especially in the areas of IT business continuity and disaster recovery, incident handling and procedures (think data breach), and computer and data security training. The message and attitude of an IT compliance function should always be that proactive activities and measures should be put in place instead of waiting for a data breach to happen.

COLLABORATION AMONG IT AUDITOR, EXTERNAL AUDITORS AND IT SECURITY

An IT compliance function can be of tremendous help to an institution's IT auditor and other outside auditors. Auditors can always come to IT compliance personnel to inquire about the areas under audit. Audit time can be saved by taking advantage of the resources that the IT compliance function may

already have for the area under audit. These resources may be especially helpful during the planning phase of an audit. At NMSU, the IT compliance officer serves as liaison with auditors because the compliance and audit functions tend to speak the same language, reducing misunderstandings. In addition, there are many areas, such as risk assessments, in which the functions can collaborate to foster the institution's well-being while avoiding duplication of effort.

To avoid unintended duplication of effort among audit, IT security and IT compliance, roles and responsibilities need to be clearly delineated, and good communication needs to exist. At NMSU, the IT compliance officer focuses on ensuring and monitoring IT regulatory compliance, but as a member of management, participates and, if necessary, develops IT policies and procedures. Audit focuses on assurance, which requires independence, and IT security focuses on implementing and monitoring technical security controls.

TRAINING AND AWARENESS

All data privacy regulations require regular training and continual awareness to ensure handlers of regulated data are aware of their responsibilities to ensure proper data protection. The IT compliance function should ensure that training and awareness are occurring and that there is appropriate documentation and tracking of the same. End users of systems containing regulated data should also be made aware of safe computing practices as it is commonly known that one's security is only as strong as the weakest link. An uninformed end user might end up defeating even the strongest technical controls. At NMSU, the IT Compliance Function very heavily stresses the importance of end user awareness at every opportunity when making presentations throughout the University community. Ensuring regulatory compliance is highly important at NMSU. Therefore, NMSU is in the process of creating an online compliance training program, which will list mandatory training for all employees, including computer and data security training.

Additionally, some laws and regulations may require specialized training to address unique requirements. Institutions should contact the applicable regulatory agency for guidance on meeting these requirements. In 2012, NMSU's IT compliance officer contacted the U.S. Department of Education inquiring about training resources, which led to discovering PTAC's resources. The PTAC offers training services free of charge to colleges and universities, and in 2012, NMSU brought PTAC officials in for a day to train faculty and staff. Over 800 employees were trained on FERPA 101 and data security as it relates to FERPA. NMSU is planning to invite PTAC back onsite to conduct more training and to perform an assessment of the University's information security practices. All universities should consider taking advantage of these PTAC services to ensure FERPA regulatory compliance and the proper protection of student data.

As IT activities in higher education have become more complex, so have the regulatory requirements and the threats to the availability, integrity and confidentiality of information.

CONCLUSION

As IT activities in higher education have become more complex, so have the regulatory requirements and the threats to the availability, integrity and confidentiality of information. Accordingly, there are countless benefits that an IT compliance function working in conjunction with audit and IT security can provide to help protect sensitive data subject to regulatory restrictions. However, these initiatives must align with the risk appetite and available resources of the institution. A formal risk assessment, for one thing, is essential. Integral also is an IT compliance function that can help ensure regulatory compliance and prevent data breaches by requiring that essential security controls are in place. Those institutions that do not have such a function may find themselves out of compliance and unprotected. Of course, IT compliance does not guarantee good information security, but it does help institutions head in the right direction for enhancing overall information security. ■

Small Shop. Big Burnout.

By Sonya von Heyking, CA, CCSA, CIA, CRMA

"I have the greatest job in the world – No day-to-day boss, no staff to manage, and complete control over my work. It's a great place to be in."

I've said this, or something close to it, at least a dozen times over the last eight years as a small shop auditor.

Whether you are the leader of a small shop or a team member, having control over your project is pretty dreamy.

I even believe the story.

After all, daily contact with one's boss makes it difficult to be perfectly at ease, even when the boss is a fantastic colleague. Managing staff is another challenge because it requires giving some of your own energy to others. Remove those factors and you remove two big workplace stress contributors.

But wait, there's more. In addition to personal autonomy, there's a healthy dose of professional autonomy. Whether you are the leader of a small shop or a team member, having control over your project is pretty dreamy. "Just leave me to my own devices and I will get this done, and done well." And by the way, there are no high-pressure deadlines on that project either. You can take the time to get it right.

Pinch me.

Considering how we traditionally characterize stress – pressure, deadlines, people issues, overtime – the life of a small shop auditor should be burnout-free.

It's not. Not even close.

DON'T BE DECEIVED BY THE ABSENCE OF TRADITIONAL STRESSORS

All the benefits of being a small shop auditor can be stressors in disguise. I stumbled upon an article on "Role Stress", a topic principally defined by Dr. Udai Pareek. It was illuminating and consoling. Many of the stressors Pareek identified not only *exist* in small shop auditing, they *define* it.

It's time to rethink stressors, to recognize and respect that the characteristics that make our modest departments attractive also wear us down. Although my modest submission isn't consistent with scholarly and scientific definitions of burnout and workplace stress there is value in applying a charitable interpretation when we look at our own environments. There is also comfort in acknowledging that, despite the seemingly perfect arrangement, we're allowed to burn out, and grumble occasionally about our perfect jobs.

Project autonomy enables small shop auditors to handle an engagement from cradle to grave. It necessarily requires shifting your focus from high level objectives to low level details and back again several times. This role fluctuation is exhausting and involves some mental gymnastics. There's something to be said for a well-defined set of tasks, or at the very least a consistent lens. If you aren't convinced, try changing the prescription in your eyeglasses every few hours and tell me how you feel at the end of the day. Although professional freedom is a joy of the job, we need to be mindful of the stress it adds and be purposeful in how we manage that stress.

Small shop auditors are required to gain proficiency in an array of technical areas – often very quickly. In a college environment, this includes medical protocols, research grant requirements,

ABOUT THE AUTHOR

Sonya von Heyking, CA, CCSA, CIA, CRMA *is the Director, Internal Audit at the University of Lethbridge in Alberta. Responsible for all internal audit activity, her diverse projects have included economic analyses of academic and research programs and activities, advisory and facilitation engagements, traditional assurance assignments, and workplace investigations. Sonya holds the Chartered Accountant, Certified Internal Auditor, Certification in Control Self-Assessment and Certification in Risk Management Assurance designations.*

Lastly, the life of a small shop auditor almost always means being the single point of contact for every aspect of an engagement.

cost accounting, student services, motor vehicle pools and myriad other specialities. While the varied competencies and skill sets can give you a boost professionally and personally, being a jack-of-all-trades *and* master of all trades takes a lot of energy. Personally, I love the endless learning of the role, but admit that one of its great benefits also contributes to a great deal of fatigue.

Lastly, the life of a small shop auditor almost always means being the single point of contact for every aspect of an engagement. You are frequently responsible for maintaining relationships with all stakeholders: internal, external, auditees, governance bodies and senior executives. Managing relationships and communication with diverse groups, who bring disparate and perhaps competing expectations requires a nimble and professional disposition around the clock. Although these relationships are often rewarding, the role ambiguity they engender is also a source of stress.

But there is a silver lining in all these stressors. The aspects of our profession that create the strain are the things we brag about at parties. It's why we shy away from complaining to our frazzled corporate friends that work is wearing us down. We love these parts of the job.

ACKNOWLEDGE, RESPECT AND TREAT STRESS

Find ways you can recharge your professional batteries. This can be as involved as a new certification, or as modest as a lunch session or online training module. Connecting with other professionals while gaining a skill set, away from the office, often provides much needed energy.

But connecting doesn't need to be centered on development. Sharing experience, advice, or just a cup of coffee can be a real infusion of energy. Find professionals near you and get together once in a while. Attending a conference usually fires me up for another six months of work just because of the social interaction. Another professional's perspective, or just another voice in the room can really turn things around when you are in a slump.

In addition to building external connections, stay in touch with auditees and other departments within your organization.

Rethink your department goals – are you working to complete the audit plan, or to effect meaningful change? Are you being fair about how you measure your role? If you perpetually feel behind, then you probably aren't acknowledging the varied demands on your time and how that affects your productivity. Consider changing your value proposition while remaining within the standards. Measure your success according to realistic goals – and pat yourself on the back once in a while.

In addition to building external connections, stay in touch with auditees and other departments within your organization. If you encourage a positive cycle of information related to audit results and process changes, those relationships might be easier to manage because they aren't always centered on the testing work. This helps develop good relationships, gets you out of the audit box, and refreshes your view of the areas you work with.

Don't put all your eggs in the work basket. It's tempting to do it all when that is your job description, but you have to engage in other activities. I run. Not well, mind you, but it allows me to be attentive to myself for a while. Find something you enjoy and allocate time to doing it without checking your email or finishing your file notes.

I'm not a stress management expert, but I am a single-person audit shop. I am also a dedicated audit leader, and a reflective professional. I hope this column can start a conversation, and if you have experiences or comments to share, then let's connect. ■

Network Security: 11 Questions Every Auditor Should Ask

By Allison MacFarlan, CISA, CISSP

Auditors are often asked to review practices around restricted areas of a campus network or to evaluate the effectiveness of IT security in a business area with specific IT control requirements. These reviews may solicit some kind of data dump from the systems that provide that security. While it is important to determine exactly what ports/services are being allowed into your restricted networks, there are other practical issues that may turn out to be more important to your overall compliance posture. In this article, we will explore the most useful questions you can pose to the security staff about devices that provide secure boundaries in your network.

We will explore the most useful questions you can pose to the security staff about devices that provide secure boundaries in your network.

Firewalls have been around since the late 1980s to provide packet and port filtering from one network to another or at an institution's borders. There are host-based software firewalls, like the Windows Firewall, the Unix iptables, ZoneAlarm Pro, and even the add-ons such as those packaged inside Symantec's Endpoint Protection. There are also firewall appliances like the Cisco PIX and ASA, Juniper and Checkpoint which are designed to inspect packets for a match to a rule-base at very high speeds and are able to track "stateful" connections, i.e., connections you initiate from inside the firewall that need to come back. Site-to-site Virtual Private Networks (VPNs) can be set up between firewall appliances. Their underlying Operating System (OS) and model determine how many simultaneous connections they can handle and the kinds of extra features, such as encryption standards, advanced management interfaces and connection speeds, they permit (e.g., 1-gig, 10-gig copper or fiber).

Network protection can also be provided by Intrusion Detection Systems (IDS), which are servers or devices that passively monitor network traffic inside or at the boundary. An IDS can be signature-based, like "Snort" (a common example), or be heuristic which means that it develops its network intelligence by analyzing network patterns over time. In university environments, it is possible to build a comprehensive IDS with open-source software and some good network "taps", as long as you have the available storage for large volumes of traffic and time to sift through and alert on it. Examples of commercial IDS appliances that gather network flows include Lancope Stealthwire, Enterasys Dragon and IBM ISS. These more expensive solutions come with a web-based dashboard that allows the security or network administrators to "see" their biggest attack sources and any inside hosts that are making lots of noise. Many of the commercial solutions also allow you to import signature-based alerts so that what rises to the top is both odd and special.

Many of the commercial solutions also allow you to import signature-based alerts so that what rises to the top is both odd and special.

An Intrusion Prevention System (IPS) is an appliance which makes decisions itself, and blocks traffic according to its rule-base. An IPS differs from a firewall in that it operates at a higher network level. It can interpret things like web URLs and malware signatures or hashes, and it has to be installed inline. It has to be connected to the router that is allowing traffic in, so it can block that traffic. Early IPS systems had the unfortunate tendency to shut down campus networks when they encountered variable traffic like BitTorrent, and they require lots of tuning if they're going to be used at the Internet border. Examples of IPS appliances include the Juniper Networks IDP, the IBM Proventia, and the Tipping Point devices. These have matured, and are more reliably blocking bad traffic and linking to ticket/notification systems.

ABOUT THE AUTHOR

Allison MacFarlan, CISA, CISSP *is the Senior Information Security Risk Analyst for Carnegie Mellon University in Pittsburgh, Pa. She coordinates IT audit work by outside auditors, and does application assessments and compliance reviews for new and existing IT projects. She has a CISSP, a CISA, and an MSIT in Information and Assurance from CMU.*

When you audit how the staff is maintaining its security infrastructure some questions are always applicable no matter what kind of system or device they have installed.

All three of the technologies identified need to be updated regularly at the OS level and in the rule-base. As hosts and networks are created and removed on your network, rules should be adjusted, and the staff will need a method or methods to keep track of these updates and the general state of the system. Record-keeping should include when ports were opened and by whom and for general exceptions made across the board for certain hosts that generate lots of traffic (like your mail servers).

When you audit how the staff is maintaining its security infrastructure some questions are always applicable no matter what kind of system or device they have installed:

1. Who has the ability to make changes to these devices, and what prompts the change?
2. What version of the underlying OS is running, and what's the latest version? Is the security staff responsible for this, or is the vendor?
3. Does the vendor have access to this device, and if so, how are they getting in?
4. Is this device visible to the university's internal network (e.g., students) or even the external network?
5. What kind of redundancy do you have, especially for firewalls and IPS devices?
6. Is it possible to tie changes to this device to any change control or ticketing system? Is Change Authority approval required for any networks filtered by this system?
7. How often do you audit your own rules for accuracy?
8. What kind of access control is used for administration, and are there different administrative roles?
9. If it's an IDS or IPS, how often do you update the rules? Do these rules come from the vendor or an open-source repository?
10. For an IDS or IPS, which rules are you disabling, and why? Is this rule-base tweaking a function of the device's location in the network or to speed up performance?
11. Where are you logging your hits, and how much of that do you keep?

In my 10 years as a security engineer I was never asked any of these questions, and I wondered why. Usually, I was asked to provide a dump of the configuration and rule-base, which is often a huge text file that the auditor has to sort by network and host and then analyze. Such analysis has its advantages, especially if the rule-base is not consistent with network policy or hasn't been updated, but it doesn't illuminate the real due-diligence required for effective network security. Your network and security people are expensive; make them do their jobs well! ■

Your network and security people are expensive; make them do their jobs well!

You Win When ACUA Wins!

ACUA has set a goal of obtaining at least 50 new member institutions in 2014. The Membership Committee will be pursuing several different tactics to obtain this goal, but ***we need your help***!

How can I help? Reach out to your friends and colleagues at non-member institutions. Tell them about the value that you find in ACUA and invite them to join. It's just that simple!

How do I know if an institution is an ACUA member? A directory of all current ACUA members is posted on the ACUA website. Simply log in to the site and search the directory located in the Member Services area.

How does an institution join? Membership applications can be downloaded from the ACUA website. Applications can be found on the Join ACUA page under the Membership menu.

What's in it for me? Prizes! The second question on the membership application asks applicants how they heard about ACUA. Ask the institution that you have invited to join to include your name on the line labeled "A Colleague". Every time that you are listed as a reference your name will be entered into a drawing for one of three prizes. The more members that you recruit; the better your chances of winning.

Prizes Include:

Prize #1 – Hotel accommodations for four nights at the InterContinental Buckhead Atlanta for the 2015 Midyear Conference **OR** four nights at the JW Marriott Indianapolis for the 2015 Annual Conference.

Prize #2 – Complimentary registration at the 2015 ACUA Annual Conference

Prize #3 – Complimentary registration at the 2015 ACUA Midyear Conference

Membership applications must be received by December 31, 2014. Only ACUA members are eligible to win prizes. ACUA Board Members are not eligible to win prizes. An individual selected in the drawing may only win one prize.