| VOLUME 57 | NUMBER 1 | WINTER 2015 |

COLLEGE & UNIVERSITY AUDITOR

PCI DSS 3.0
RAISES DATA RISK MANAGEMENT BAR FOR UNIVERSITY AUDITORS

LEARNING TO DO MORE WITH LESS IN A SMALL AUDIT SHOP

ACUA
ASSOCIATION OF COLLEGE & UNIVERSITY AUDITORS

INSIDE:

IDEA
Data Analysis Software

Isn't It About Time.

Time. We need more of it.
Technology should help not hinder the quest for time, but it must be both easy to use and yield high-quality results.

IDEA® Data Analysis empowers you to achieve more in less time.

- Reduce audit time by 20-50%
- Increase efficiency with unlimited support and free resources
- Conduct more thorough audits by analyzing 100% of data
- Automate repeatable tasks without programming

It's About Time to Use IDEA

ACUA Strategic Partner
Exclusive Discounts & Benefits

- Preferred pricing on IDEA and license renewals
- Training discounts
- Special hands-on session at the Mid-Year Conference

Contact us to see IDEA in action.
888.641.2800 • sales@audimation.com • audimation.com

WINTER 2015
COLLEGE & UNIVERSITY AUDITOR

CONTENTS

FEATURES

COMPLIANCE

COLUMNS

AUDIT TOOLS

FRAUD

LEADERSHIP

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.

Editor
Sam Khan, Oregon State University
sam.khan@oregonstate.edu
541-737-7336

Editing Staff
Amy Hughes, Michigan Tech
David Dixon, Governors State University
Mary Ann Mackenzie, Auburn University
Sterling Roth, Georgia State University

ACUA Management
Stephanie Newman, *Executive Director*
Raven Hardin, *Association Manager*

Upcoming Deadlines
Summer 2015 Issue – June 1, 2015
Fall 2015 Issue – August 31, 2015

College & University Auditor is the official publication of the Association of College & University Auditors. It is published three times a year as a benefit of membership. Articles in *College & University Auditor* represent the opinions of the authors and do not necessarily represent the opinions of governance, members or the staff of the Association of College & University Auditors. Acceptance of advertising does not imply endorsement by ACUA. ©2014 Association of College & University Auditors.

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

LETTER FROM

THE EDITOR

By Sam Khan
Editor

"Get wisdom as cheaply as you can," writes Russell Eubanks in a recent post on the Internet Storm Center blog. I couldn't agree more. He adds, "I was encouraged to learn from the mistakes of others as a means to avoid the full pain of what they were forced to experience." This is great advice that can be applied to the work of an internal auditor.

"Payment card data remains one of the easiest types of data to convert to cash, and therefore the preferred choice of criminals."

What lessons can we learn about the numerous high-profile data breach cases that occurred in 2014, many of which involved credit card data, and how can we share this valuable information with our organizations to reduce the likelihood and impact of a data breach?

This is a great time to review the risks related to credit card processing at your organization, and whether the controls in place comply with the new Payment Card Industry Data Security Standard (PCI DSS 3.0), which became mandatory on January 1, 2015.

Author Jeff Sanchez provides an overview of those changes, and provides action items for university auditors to ensure a smooth transition to the new standard in *PCI DSS 3.0 Raises Data Risk Management Bar for University Auditors (page 4).*

"Payment card data remains one of the easiest types of data to convert to cash, and therefore the preferred choice of criminals," according to the *Verizon 2014 Payment Card Industry (PCI) Compliance Report.* The report states that 74 percent of attacks on retail, accommodation, and food services companies target payment card information.

In addition, the report points out that only about one in ten organizations were fully compliant with PCI DSS 2.0 at the time of their baseline assessment. What does this mean for the rate of compliance with PCI DSS 3.0, which adds more requirements?

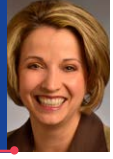
The PCI Security Standards Council has stated that the changes in DSS 3.0 are designed to, "help organizations take a proactive approach to protect cardholder data that focuses on security, not compliance, and makes PCI DSS a business-as-usual practice." The key themes are improving education and awareness, increasing flexibility, and viewing security as a shared responsibility.

This theme of security as a shared responsibility is also contained in *Cybersecurity: What the Board of Directors Needs to Ask,* which states that the board has a role to play in securing sensitive data. While senior management should be addressing the challenges to secure sensitive data directly, with auditors reviewing their work, the board should be scrutinizing the quality of cybersecurity planning. For example, the board should require that internal auditors perform an annual "health check" of the organization's cybersecurity program, and board members should meet with the chief information security officer at least annually.

I want to thank the authors who contributed their time and expertise to make this issue possible. If you have an article idea or know someone whose knowledge would benefit our members, please call or email me at 541-737-7336 or sam.khan@oregonstate.edu. ■

LETTER FROM

THE PRESIDENT



By Sandy Jansen
President

I believe that ACUA is the most valuable resource available to audit and compliance professionals in higher education. As I consider our core values—those guiding principles by which we operate—I am reminded of all the great work to keep those values alive. ACUA's core values are

I believe that ACUA is the most valuable resource available to audit and compliance professionals in higher education.

- integrity
- open sharing of knowledge
- mutual trust and friendship
- respect
- commitment to excellence
- innovation

To continue to be the most valuable resource, the association's committees have taken action to address our goals while ensuring the work aligns with our core values. They have already achieved success and continue to work to advance our organization.

The External Relations and the Internal Audit Awareness Week are two active committees dedicated to integrity and commitment to excellence.

- The External Relations Committee has been working with ACUA volunteers to reach out to other organizations, including the Association of Governing Boards (AGB) and the National Association of College and University Business Officers (NACUBO), to advance internal auditing. ACUA continues to collaborate with the University Risk Management and Insurance Association (URMIA), Association of Healthcare Internal Auditors (AHIA), and the Society of Corporate Compliance and Ethics (SCCE). The focus of this committee is outreach to other organizations.
- The Internal Audit Awareness Week Committee has some exciting plans to help all of us build awareness on our campuses. As an added bonus, Julia Hann of Georgia College has been engaging new volunteers to assist in these efforts. It's great to have new volunteers helping on such an important initiative. The committee has a surprise in store for our members later this spring.

The Best Practices Committee is dedicated to open sharing of knowledge. It completed the *2014 Salary and Resource Survey,* which is available for all members on the Members Resources page of the ACUA website. Thanks for participating in this survey and for helping to develop a resource for our members. I know many of our members use this resource for benchmarking purposes.

In addition to open sharing of knowledge, the ACUA Communities taskforce builds on the values of mutual trust and friendship as well as respect. Don't forget to get involved in the new ACUA Communities! This online networking opportunity provides ACUA a much-needed update of older technology. Communities will continue to tie us all together as we reach out to one another for advice and ideas. We all can be part of ACUA's story by sharing on ACUA-C.

Finally, ACUA believes in innovation, and our webinars continue to be one of the greatest benefits ACUA offers. The webinars are free and provide an hour of continuing professional education. The information is timely, on target, and helps our members address critical areas and risks in higher education. Best of all, members are able to attend from the comfort of their offices. I love technology. If you have not attended one, look for the next offering. We continue to receive great feedback. Thanks to Baker Tilly for collaborating with ACUA to offer four of these webinars each year.

As always, I encourage you to be part of ACUA's story and volunteer your time and talents to continue to move ACUA forward. Our members are the lifeblood of this organization.

Thank you in advance for your service and for adding your face to ACUA's story! ■

Sandy

PCI DSS 3.0 Raises Data Risk Management Bar for University Auditors

By Jeff Sanchez

Institutions of higher learning strive to foster an open and welcoming atmosphere and create fertile ground for learning and creativity. Unfortunately, this environment also invites hackers, who target colleges and universities as rich and easily accessible sources of credit card data, Social Security numbers and intellectual property.

Unlike retailers, which have the ability to maintain tight control over network access, academic networks are designed to accommodate access from all kinds of devices at any time and from anywhere around the globe. This exposes these institutions to unique risks, as any terminal capable of accepting a payment or accessing a payment system is a potential hacker penetration point.

Any terminal capable of accepting a payment or accessing a payment system is a potential hacker penetration point.

Complicating the picture is the fact that, unlike other professional environments where training can play a significant role in threat reduction, colleges and universities deal with an amorphous group of users, including students used to indiscriminate file sharing—an ideal demographic for hackers seeking to borrow a "key" from a legitimate user to gain access to the network for nefarious purposes.

EMERGING THREATS

Most people tend to think of hackers as villains breaking into a system; however, fraudsters these days are more likely to steal the keys of legitimate users to gain access. Typically, this is done with broadcasted "phishing" emails containing password-stealing malware, sophisticated "spear phishing" campaigns targeting top executives with personalized phishing emails, and "watering hole attacks" in which a secure server is targeted with malware planted on a less-secure network likely to be frequented by users logged into the secure network.

To address these emerging threats, the Payment Card Industry Data Security Standard (PCI DSS) was updated, effective Jan. 1, 2014. It officially replaced PCI DSS 2.0 (Version 2) on Jan. 1, 2015. For auditors and IT risk managers, this deadline means they have to up their game to comply with the new standard.

VERSION 3 OVERVIEW

PCI DSS applies to all organizations that accept, transmit or store any cardholder data. The latest version, PCI DSS 3.0, or Version 3, has three aims:

1. Provide compliance guidance and clarity
2. Align security standards with emerging threats
3. Establish data security as a continuous practice instead of a one-time snapshot

In Version 3, the changes are designed to give organizations a strong but flexible security architecture with principles that can be applied over a wide range of technology, payment and

ABOUT THE AUTHOR

Jeff Sanchez *is a Managing Director at Protiviti and leader of the firm's PCI Data Security Standards practice. Jeff works with large organizations to address cyber threats and reduce the efforts associate with PCI compliance through the design of secure payment processes and security architecture. Jeff is a Certified Internal Auditor and a PCI PA-QSA.*

business environments. The changes were made to address several core weaknesses and challenges that have emerged from prior data breaches. Specific change drivers include:

The changes were made to address several core weaknesses and challenges that have emerged from prior data breaches.

- A lack of awareness and education about the PCI standard and its security requirements and objectives
- Weak passwords and authentication
- Third-party security challenges
- Slow detection of breaches and malware
- Inconsistency in PCI compliance assessments

Version 3 includes five new requirements, which became effective on Jan. 1, 2015:

1. Unique authentication credentials for service providers with access to the cardholder data environment
2. Tamper protection for point-of-sale devices
3. Penetration testing
4. Detection of broken authentication sessions—a new addition to the Open Web Application Security Project (OWASP) Top Ten vulnerabilities list and to PCI DSS 3.0
5. Additional data security requirements for third-party service providers

SEGMENTATION

Most organizations that need to comply with the PCI DSS have invested a significant amount of time and energy in defining which systems must meet PCI DSS requirements. This process of separating critical data systems from other information technology is called segmentation. Any system, component or device with even a remote chance of accessing confidential data is subject to PCI DSS, or "in-scope."

To assess segmentation, penetration testing, or controlled hacks, must be conducted from all out-of-scope components to verify that there is no way they can be used to access sensitive data. In other words, to be considered out of scope for PCI DSS, an organization must demonstrate that a breach in an out-of-scope segment (including a breach of administrative accounts) does not allow an attacker to compromise the cardholder environment.

Any system, component or device with even a remote chance of accessing confidential data is subject to PCI DSS, or "in-scope."

In Version 3, the definition of system components has also been expanded to include hosted payment pages and redirection servers that use direct post or Java script technologies. Under Version 2, it was possible to "de-scope" Internet-facing systems by outsourcing the online payment page to a third party. Under the new standard, many of these third-party servers and systems fall in scope because attackers have found ways to access cardholder data through them.

The only "out" for organizations that cannot ensure the security of web servers internally is to fully outsource the web infrastructure.

SCOPE REDUCTION STRATEGIES

As the bar for segmentation is raised, companies are looking for solutions that will help them manage their in-scope systems better. One scope reduction strategy that is becoming more valuable under Version 3 requirements is point-to-point, or end-to-end, encryption. More and more payment systems are moving toward this full encryption technology in which credit card information is encrypted at the point of sale and decrypted only within the protected confines of the payment gateway.

POINT-OF-SALE SECURITY

In response to recent attacks in which point-of-sale (POS) devices had been physically modified to capture cardholder data, Version 3 includes a new set of control requirements around physical security for POS devices.

First, merchants must maintain an inventory of POS devices, which must be identified in detail, including the location and serial number of each device.

In addition, POS devices must be inspected periodically for tampering, and employees at POS locations must be trained in how to detect and prevent device tampering.

Next steps

Four Things University Auditors Should Do Right Now

1. Be aware; changes are here.
2. Check for compliance gaps, especially with regard to the scope/segmentation changes in Version 3.
3. Monitor the Payment Card Industry Security Standards Council website for information supplements and other updates.
4. Ask your Qualified Security Assessor for an interpretation of the new segmentation rules and each new information supplement.

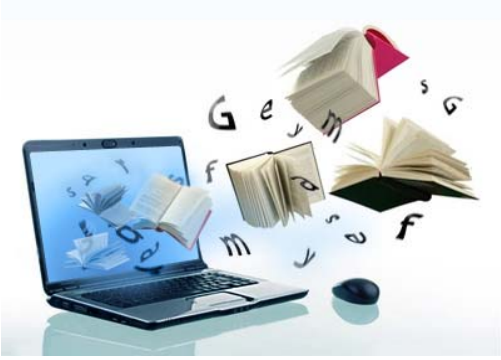
CONCLUSION

The changes reflected in PCI DSS 3.0 are likely to result in significant additional work for college and university auditors, as well as IT departments and risk managers. It is especially important that auditors understand the risks and work with stakeholders to ensure that effective data security measures are in place, including a written and fully rehearsed response plan to cyber attacks.

Universities still working on complying with Version 2 should shift their efforts to Version 3 as soon as possible. Organizations that rely on third parties to handle any aspect of their IT and customer data environment need to document roles, responsibilities and accountabilities for security and make sure their third-party partners are Version 3-compliant.

Taking steps now to implement the new rules effectively can help institutions to ensure better protection of personal payment information and avoid serious reputational harm caused by unauthorized exposure of valuable research or students' academic, health or credit card data. ■

ASSOCIATION OF COLLEGE & UNIVERSITY AUDITORS



What is the ACUA Risk Dictionary?

The ACUA Risk Dictionary is a comprehensive database of risks and their associated controls for areas specific to higher education. Higher Education audit departments can use the risk dictionary for identification of an audit universe specific to higher education which can be used for performing their annual risk assessments and preparing their annual audit plan.

The ACUA Risk Dictionary can also be used to prepare project level risk assessments for areas such as:

- NCAA Compliance
- Student Financial Aid
- Export Controls
- Research Compliance and many more!

After having identified the risks for your audit project, the ACUA Risk Dictionary contains the associated controls which can then be used to prepare an audit program to test whether the proper controls exist.

Is the ACUA Risk Dictionary for YOU?

Business officers, risk officers, compliance officers and other higher education leadership can use the ACUA Risk Dictionary to provide a comprehensive list of areas that could likely need their attention. For someone new to their position or new to higher education, the ACUA Risk Dictionary will be especially beneficial in identifying not only broad areas where inherent risks are common, but also specific risks within those areas and their associated controls.

In the absence of a formal risk management structure, the ACUA Risk Dictionary provides a concrete and comprehensive starting point for identifying, evaluating, and managing risks across the organization.

You now have the ability to submit new risks and controls for the dictionary. The Risk Dictionary is a living document, so check it out with an eye toward what you can contribute.

The ACUA Risk Dictionary is available for *FREE* as a benefit of ACUA membership or by subscription to non-members.

Procurement Challenges in the Government-Funded University and Research Environment: *Counteracting Noncompliance*

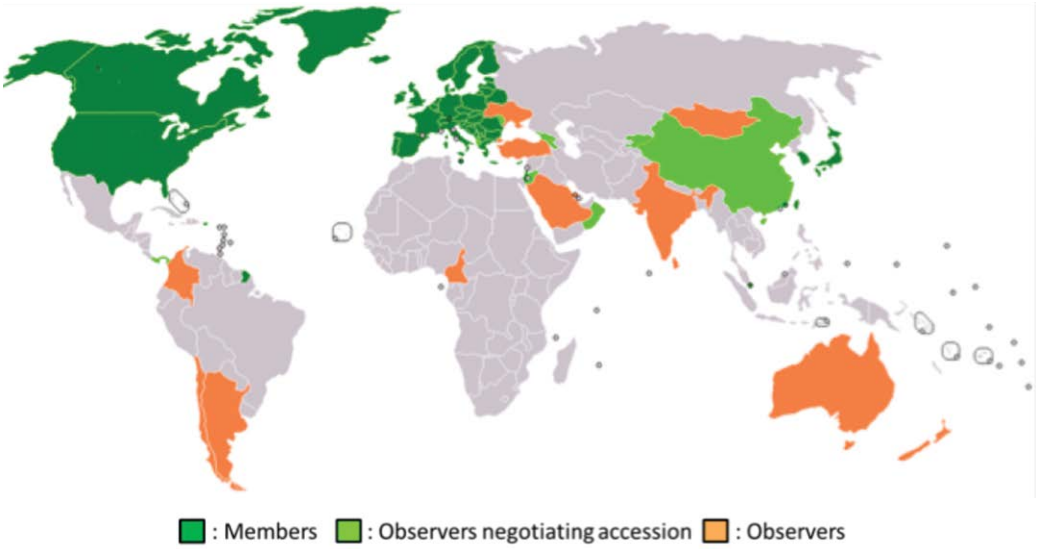
By Patrick Graber and Sylvia Föry

Public institutions in countries which ratified the Agreement on Government Procurement (GPA) have to follow the specific rules of the corresponding national framework for public procurement. Accordingly, public-funded universities and research institutes in these countries must also follow these rules. In addition to negative media exposure and resultant reputational damage, noncompliance can lead to project postponements due to legal appeals, misappropriation of monetary resources due to uneconomical prices, and corruption and fraud. The latter outcomes especially may result in a decrease in sponsoring agencies' willingness to fund.

LEGAL FRAMEWORK

The GPA, a binding international treaty, was signed on April 15, 1994, at the same time as the Agreement Establishing the World Trade Organization (WTO) and entered into force on January 1, 1996. The initial members are Austria, Belgium, Denmark, Finland, France, Germany, Greece, Ireland, Italy, Luxemburg, the Netherlands, Portugal, Spain, Sweden and the United Kingdom (all members of the European Union) as well as Israel, Japan, Norway, Switzerland and the United States of America (USA). As of today, 43 countries have signed the GPA.

Figure 1: Member Countries



The main objective of the GPA as stated in its preamble is to define "an effective multilateral framework of rights and obligations with respect to laws, regulations, procedures and practices regarding government procurement with a view to achieving greater liberalization and

ABOUT THE AUTHORS

Patrick Graber *is the Chief Audit Executive of the Board of the Swiss Federal Institutes of Technology (ETH Board). He holds a Master of Science in Business Administration and a Master of Law and is a Certified Internal Auditor.*

Sylvia Föry *is a Senior Auditor at the Board of the Swiss Federal Institutes of Technology (ETH Board). She holds degrees in business administration and business information technology. She is a Certified Internal Auditor and a Certified Information System Auditor.*

In addition to negative media exposure and resultant reputational damage, noncompliance can lead to project postponements due to legal appeals, misappropriation of monetary resources due to uneconomical prices, and corruption and fraud.

expansion of world trade and improving the international framework for the conduct of world trade."

This article focuses primarily on the Swiss legal framework, but the issues addressed will also apply to other national frameworks. In addition to the GPA and a certain number of bilateral agreements, primarily with the European Union, Switzerland has legislated a special submission law for public procurement by public authorities as well as complementary regulations at the national level. In addition, the cantons (similar to the USA states) have their own legislation for public procurement.

CONDITIONS AND THRESHOLD AMOUNTS

To decide if and how a specific procurement has to be treated according to the rules of the legal framework for public procurement, four criteria have to be considered:

- Does the purchaser (public authority) have to comply with the submission laws?
- Is the item to be purchased listed among the goods or specific services of the submission laws/ GPA agreement?
- Is the price (value) above the threshold amount (see table below)?
- Do any exceptions apply?

The following table shows the relevant threshold amounts for a WTO tendering.

Category	Switzerland (CHF)	USA (USD)	European Union (EUR)
Goods	230,000	$204,000	207,000
Services	230,000	$204,000	207,000
Construction	8,700,000	$7,864,000	5,186,000

If the criteria are met and there is no exception, a WTO tendering with an open call for tender has to be performed. However, the Swiss regulation for public procurement by public authorities allows avoiding the obligation of an open call for tender if any of the following exceptions apply:

- No acceptable tender (no tenders received, no vendor fulfills the qualification criteria, no fulfillment of technical specifications, collusion)
- Only one supplier due to technical specification requirements, intellectual property or objects of arts
- Emergency purchase due to unforeseeable events
- Prototyping in relation to research
- Subsequent procurement for an additional phase of construction work
- Replacements/upgrades can only be done by the initial supplier
- Purchases at auction exchanges
- Winner of a contest with independent jury
- Purchases at time-limited extra favorable prices (liquidations)

PROCUREMENT PROCEDURES

The legal framework provides different procedures depending upon whether the specific procurement exceeds threshold amounts (Procedure by Law, WTO tendering) or not (Procedure by Regulation).

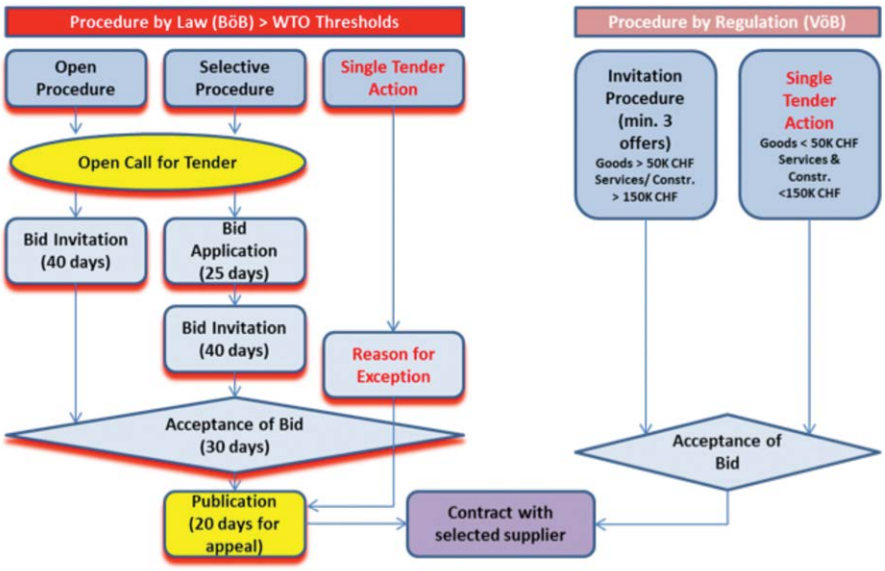


Figure 2: Procurement Procedures

The Procedure by Law provides for either the "open procedure," the "selective procedure" or the "single tender action." The open procedure and the selective procedure are quite similar and both begin with an open call for tender published on a dedicated electronic platform. While the open call for tender of the open procedure refers to the whole procurement and allows everybody to submit a bid, it only contains the choice of the tenderer in the selective procedure. This additional step allows restricting the circle of the potential tenderers according to predefined criteria. In the subsequent bid invitation, only the selected tenderers can submit a bid. The other steps are similar.

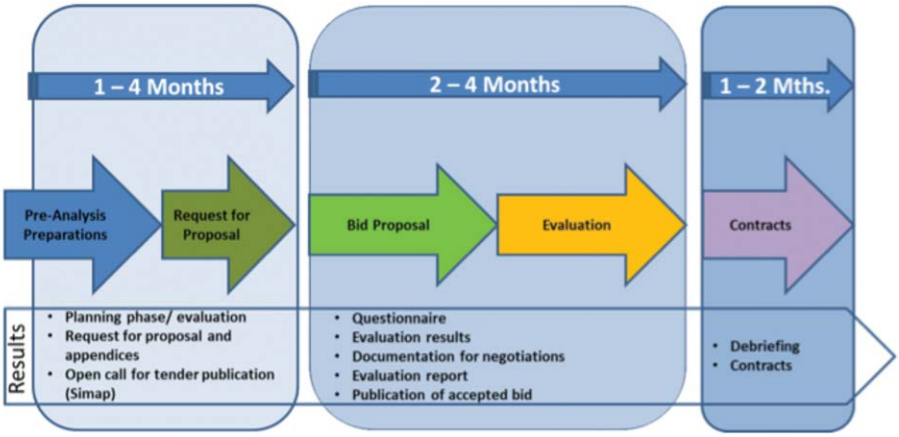


Figure 3: Time Horizon for a WTO Tendering

When one of the exceptions foreseen by the regulation applies to the selected procurement, the consideration of only one tenderer is allowed (single tender action). The reason for the exception must be clearly justified. All procedures by law end with the publication of the acceptance of bid on the electronic platform.

In the Procedure by Regulation, a minimum of three tender offers are requested depending on the amount and the category of the specific procurement. No publication on the electronic platform is required.

SPECIFIC TOPICS FOR RESEARCH AND TEACHING

The legal framework was developed for government procurement generally. Teaching and research institutions have particularities, especially within highly specialized research environments, which can impact the selected procurement procedures. Some of these particularities are:

- Lack of market
- Prototyping
- Co-development with research partner
- Sponsoring
- Funding
- In-house development and spin-off
- Restricted know-how
- Relationships among researchers and industries
- Time horizon in a competitive research environment
- Research/business secrets and innovation
- Intellectual property

AREAS OF NONCOMPLIANCE

During procurement audits, five main areas of noncompliance have been identified, as described below:

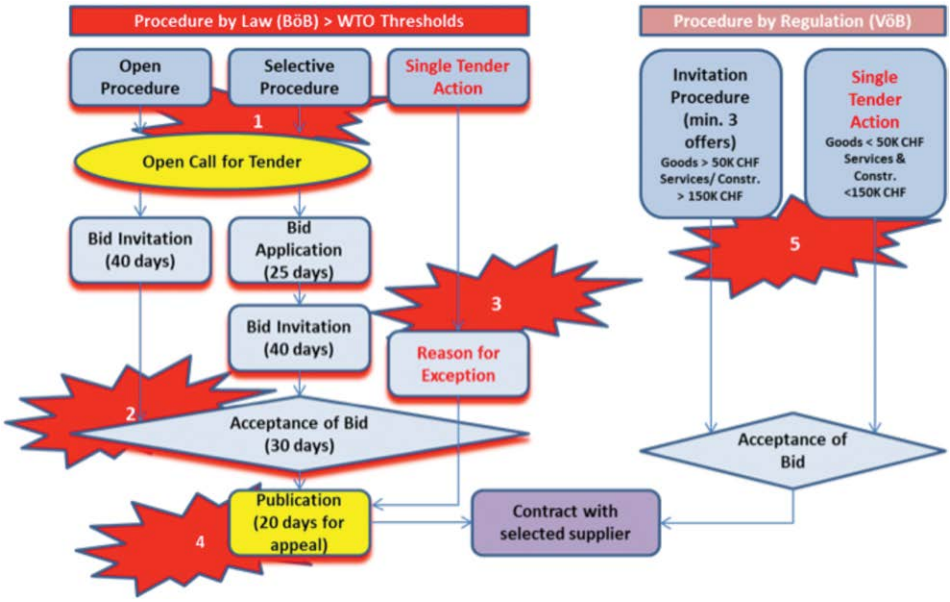


Figure 4: Principle Areas of Noncompliance

1. Open Call for Tender: The principal issues were an insufficient market analysis, prior involvement of suppliers warranting a need for a market analysis, missing or inadequate requests for proposal, splitting orders to avoid a WTO tendering and bias/conflicts of interest.
2. Acceptance of Bid: In addition to prior involvement of suppliers and bias/conflicts of interest, other principal issues here were missing or incomplete logs of bids received, non-reproducible or erroneous evaluations, inadequate weighting of price criteria, selective negotiations and unjustified break offs.
3. Reason for Exception: In spite of the requirement that every exception be clearly justified, missing justification and utilization of an inapplicable exception rule were identified. Also found was order splitting.

4. Publication of Accepted Bid: Issues here were missing publication for the single tender action and requests for debriefings/legal appeals.
5. Single Tender Action Instead of Invitation Procedure: The main findings in this area concerned insufficient market analysis, missing request for proposal, order splitting, bias/conflicts of interest, and requesting fewer than three offers.

Such noncompliance presents challenges and calls for counteractions, such as assuring:

- Comprehensive planning and bundling of purchases (replacements, maintenance, services, potential options, etc.), including new professorships with initial funding and overseeing existing contracts (framework contracts).
- Strong knowledge of public procurement procedures and requirements (choice of the best procedure, transparency, equal treatment and nondiscrimination among vendors).
- Evaluation based on predefined criteria involving, if necessary, a prior market analysis and adequate requests for proposal with appropriate criteria, including vendor and technical specifications.
- Collaboration between the decentralized requestor and the centralized purchasing department that incorporates insights into technical specifications, context and research environment.
- Complete and understandable evaluation documentation that will withstand requested debriefings from disregarded suppliers and legal appeals.
- Awareness of bias and conflicts of interest and if existing, putting restrictions on involvement in procurements.
- No signing of the contract with the considered supplier until the legal period for administrative appeal is over.
- Agreement for right of inspection of the bid calculation when the total amount exceeds 1 Mil. CHF (due to lack of competition).

AUDIT PROCEDURES

Procurement audits should consider strategy, the procurement process, organization, responsibilities and controls. Because most purchases are initiated by decentralized units, different approaches may be needed. For example, topics regarding procurement in faculty audits might not be addressed in other audits. Across the board, however, audits of internal control systems should determine if effective controls are in place to avoid noncompliance in the procurement process.

IMPACTING CHANGE

Procurement may not receive the same management attention as core teaching and research processes in public-funded universities and research institutes. However, proper purchasing strategy and processes are vital to the success of those core processes. Impacting change calls for procurement responsibilities and internal controls that are well defined in policies and clearly communicated. Periodic training and education are also essential to increase and reinforce knowledge of public procurement requirements. Thus change will have an impact in continually increasing awareness of possible corruption or fraud, enabling effective and compliant purchasing actions, and assuring economy of operations and a positive institutional reputation. ■

---

[1] See World Trade Organization (http://www.wto.org/english/tratop_e/gproc_e/gp_gpa_e.htm)

[2] Preamble to Agreement on Government Procurement, April 15, 1994

Wolters Kluwer
Audit, Risk & Compliance

TeamMate® Analytics

Data analysis for every audit

Integrates with TeamMate Audit Management System and available for standalone use

Start your 30-Day Trial today at
TeamMateSolutions.com/Trial

POWERED BY:
topcaats

Copyright © 2014 Wolters Kluwer Financial Services, Inc. All Rights Reserved. 3936

Learning to Do More with Less in a Small Audit Shop

By Robert Berry

Expectations have never been higher for internal auditors. We are expected to be risk managers, compliance partners, proper accounting advocates, the occasional therapist and friendly adviser. At its most basic level, the job of an internal auditor is to inform stakeholders whether or not management's processes effectively reduce negative risk and/or increase positive risk.

Stakeholders are expecting deeper levels of evaluations and affirmations from assurance providers.

The complexity of modern organizations has made it more difficult to identify, evaluate and report risk conditions. Most modern organizations cater to one primary industry and multiple sub-industries. Many deliver multiple products and/or services.

For example, those of us in higher education have dormitory facilities, on campus dining, endowments, research, and athletic operations. This means that we serve the rental housing industry, quick serve (fast food) industry, and the investment industry to name a few.

Because of this new complex operating environment, stakeholders are expecting deeper levels of evaluations and affirmations from assurance providers (internal auditors, compliance professionals,). This can be particularly challenging for small internal audit departments. There is absolutely no way we can know everything and audit every area within the operating environment. Therefore, it is essential that we make the most effective use of the resources at our disposal.

What follows is a four step process that will help bring out the best in your small internal audit function.

STEP 1 – DETERMINE THE EXPECTATIONS

Seven years ago, I inherited a small internal audit shop (one director and one senior auditor) from a skilled audit professional. The strategy he implemented at the time involved performing many consulting services, a few high-level audits, and even fewer in-depth audits. This strategy was undertaken primarily because of the size of the staff compared to the risk in the operating environment.

At my first audit committee meeting, committee members expressed concern over the number of internal audits performed compared to the consulting services and investigations. Up to this point, I thought the level of activity produced by my predecessor was appropriate given the size and knowledge level of the department.

Therefore, I asked one simple question, "What are your expectations for this department?" The answer was; "To do more full blown audits." They further explained that they did not want the department to perform any consulting services. So I next asked, "What does an internal audit mean to you?"

The committee disclosed that, in their opinion, the purpose of audits was to give them some comfort that management was doing what it was supposed to do. Fair enough. As stated earlier, we provide reasonable assurance as to whether or not management's processes effectively reduce negative risk and/or increase positive risk. So what happened next was a healthy discussion on internal audits, consulting engagements, and investigations. We discussed the purpose of each engagement type, time commitment involved and nature of reporting.

ABOUT THE AUTHOR

Robert Berry, ACUA Board Member-at-Large, *is the Director of Internal Auditing at the University of North Florida. He holds a Bachelor of Science degree in Accounting from Auburn University at Montgomery. He is also a Certified Public Accountant, Certified Internal Auditor, Certified Information Systems Auditor and a Certified Compliance and Ethics Professional.*

They were not aware that these other "non full audit" engagements still provide some level of assurance regarding management's operating environment. We eventually came to an agreement that a good mix of all of these engagements was indeed a good course of action.

This was a very good start in managing the expectations for my small internal audit shop. Determining the audit committee's expectations led to providing education which eventually led to better decision-making.

But we weren't done yet. We still needed to determine what constituted a "good mix" of internal audit, consultant, and investigation services. Therefore, our small internal audit department needed to assess its resources and resource limitations.

STEP 2 – ASSESS THE LIMITATIONS

We began the painstaking task of performing an internal time allocation analysis. Using historical figures, we were able to determine the amount of time spent on projects and the value added per project type. On average, there were more control concerns in full audit engagements, however, there was more risk coverage in smaller engagements and consulting services. Furthermore, the quick audits and consulting engagements allowed us to focus on specific risks across the entire organization.

This exercise led us to another realization; the head of our tiny department of two, although a seasoned risk, audit and compliance professional, had no higher education industry experience. This alone could increase the amount of time allocated to projects. Therefore, we needed a creative solution to address this limitation.

As the department head, I immediately became active in the Association of College and University Auditors (ACUA). Additionally, I attended College Business Management Institute (CBMI). CBMI is a three-year higher education immersion program that walks participants through the "business" of higher education. Both of these resources proved to be essential in turning this limitation into a strength.

STEP 3 – INVEST IN SOME AUTOMATION

What was also clear was that no one, including the stakeholders, understood what to expect in the execution of delivering audit services.

After determining the expectations and assessing time and knowledge limitations, it also became clear that some tasks were not being performed efficiently. The vast majority of the department's tasks were manually performed, which is not unusual for a small internal audit department. However, automation would allow us to allocate valuable time elsewhere. We hired a computer science Federal Work-Study student to build a time and issue tracking system. This reduced the amount of time previously devoted to filling out Excel worksheets. The success of this project led to a partnership in which the information technology department designed, developed and deployed a web-based audit management system. This system added automated follow up capabilities. While this is still in the early stages of development, we are hoping to see significant time savings.

STEP 4 – SET REALISTIC EXPECTATIONS

Also at that first audit committee meeting, it was clear that we did not meet stakeholder expectations. What was also clear was that no one, including the stakeholders, understood what to expect in the execution of delivering audit services. The audit committee knew that it wanted to be comfortable with management's processes. The also knew that an independent function, such as internal auditing, could provide objective evaluations. There are, however, numerous unknowns which form the basis for audit committee opinions and expectations. These include the following:

- Number of human resource hours available,
- Industry knowledge within the department,
- Ability to obtain industry knowledge,
- Compensation compared to market,
- Level of automation,
- Amount of management support.

As an internal audit director, it is my responsibility to educate audit committee members so that expectations and resources are known, examined and adjusted accordingly.

Many times audit directors will take on more responsibility without seeking clarity, providing education and finding balance. Therefore, most small internal audit shops are continuously overwhelmed.

CONCLUSION

This article started by identifying the increasing expectations for internal audit functions. Many times audit directors will take on more responsibility without seeking clarity, providing education and finding balance. Therefore, most small internal audit shops are continuously overwhelmed.

So what happened in this small internal audit shop after (1) determining the expectations, (2) assessing the limitations, (3) investing in automation and (4) setting realistic expectations?

In the years following this initial audit committee meeting, we have grown the department by one, implemented a client driven risk assessment process, purchased a data analysis system, and provided a healthy (and agreed upon) mix of audit services. Now we all understand the expectations within the context of our resources and limitations. ■

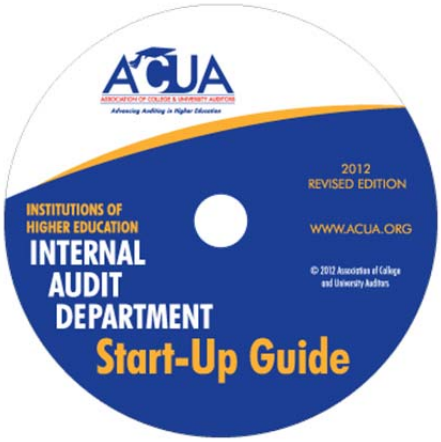
ASSOCIATION OF COLLEGE & UNIVERSITY AUDITORS

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.

Using Data for Fraud Deterrence and Detection in the Higher Education Industry

By Jeremy Clopton

Fraud in higher education takes many forms, from asset misappropriation to financial statement fraud. According to the Association of Certified Fraud Examiners' *2014 Report to the Nations on Occupational Fraud and Abuse*, the average organization loses 5 percent of its revenues to occupational fraud. Factor in waste, abuse and fraud committed by those outside the organization and the risk of losses increases further. These issues make it more important than ever for higher education institutions to consider data analytics in their anti-fraud controls.

Using data analysis was associated with a near 60 percent reduction in median fraud losses and a 50 percent reduction in median scheme duration in the cases studied.

DATA ANALYTICS AS AN ANTI-FRAUD CONTROL

Many higher education officials wonder what they can do to prevent fraud from occurring in their organizations. After all, a determined employee can be very difficult to stop. It is unrealistic to think all frauds are preventable, but there is almost always more that higher education institutions can do to reduce fraud risk in key areas.

According to the Report, the most effective anti-fraud control is "proactive data monitoring and analysis" (data analysis). Using data analysis was associated with a near 60 percent reduction in median fraud losses and a 50 percent reduction in median scheme duration in the cases studied. In addition, the data analysis process is also inherent in two of the most common methods of fraud detection: management review and internal audit. For these reasons and given the growing volume of data generated by organizations each day, it is important to know how to use data analysis to deter and detect fraud.

COMMON SCHEMES IN HIGHER EDUCATION

Proper application of data analysis for fraud detection and deterrence requires first understanding the various types of schemes committed within the realm of higher education. Figure 1 contains the six most common schemes in the higher education industry according to the Report.

Figure 1

Scheme	Definition (according to the Report to the Nations)
Corruption	A fraud scheme in which an employee misuses his or her influence in a business transaction in a way that violates his or her duty to the employer in order to gain a direct or indirect benefit.
Billing	A fraudulent disbursement scheme in which a person causes his or her employer to issue a payment by submitting invoices for fictitious goods or services, inflated invoices or invoices for personal purchases.
Expense Reimbursements	A fraudulent disbursement scheme in which an employee makes a claim for reimbursement of fictitious or inflated business expenses, e.g., filing a fraudulent expense report, claiming personal travel or nonexistent meals.
Skimming	A scheme in which an incoming payment is stolen from an organization before it is recorded on the organization's books and records.

ABOUT THE AUTHOR

Jeremy Clopton *is a Senior Managing Consultant in BKD, LLP's Forensics & Valuation Services division, specializing in the use of data analytics for fraud prevention and detection. He is a CPA, Certified Fraud Examiner (CFE) and ACL Certified Data Analyst (ACDA).*

Cash on Hand	Any scheme in which the perpetrator misappropriates cash kept on hand at the victim organization's premises, e.g., stealing cash from a vault.
Payroll	A fraudulent disbursement scheme in which an employee causes his or her employer to issue a payment by making false claims for compensation.

APPLICATION OF DATA ANALYSIS

Using these scheme definitions, we can identify the largest fraud risks: vendor management, disbursements, cash and payroll. Some of the most common analysis techniques in each of these areas are addressed below.

- **Vendor Management** – Many times, corruption and billing schemes occur through the vendor file. Looking for potential related parties or conflicts of interest by comparing employee and vendor files based on key attributes—e.g., name, address, phone or taxpayer identification number—may help identify questionable vendors. Other beneficial analyses include comparison of employee and student financial aid files, geospatial analysis of vendors to identify those located in residential areas, identifying vendors using a mailbox service and identifying vendors without an address or some variation of "hold for pickup."

Perhaps the most effective analysis technique related to disbursements is trend analysis, focused on the identification of accelerating patterns of activity.

- **Disbursements** – Billing and expense reimbursement schemes are both fraudulent disbursement schemes. In addition, corruption schemes typically involve disbursement. Perhaps the most effective analysis technique related to disbursements is trend analysis, focused on the identification of accelerating patterns of activity. Other common analytics include identifying checks issued on weekends or holidays or in round thousand dollar increments.
- **Cash** – To detect skimming and cash on hand schemes, consider focusing analytics on monitoring trends related to cash balances, voids, refunds or "no sale" transactions, particularly in bookstore, event ticket sales or other retail arms of the institutions that collect significant funds.
- **Payroll** – Ghost employee schemes work in much the same way as a fictitious vendor scheme, and they begin with employee setup. Analyzing new employee attributes compared to other active employees may help identify a potential ghost employee. Other useful analyses include monitoring employee overtime trends, identification of payroll payments without tax withholdings and analysis of manual payroll checks.

CONCLUSION

While data analysis can be a most effective anti-fraud control, it is not enough to deter and detect fraud by itself. The most effective fraud prevention program combines multiple elements to create an environment where fraud is less likely to take root. In addition to data analysis, it is important to explore other anti-fraud controls you could implement in your institution. The Report contains information regarding other anti-fraud controls to help deter and detect fraud in your institution. As you assess fraud risk in your organization, be sure to evaluate all possible anti-fraud controls. Where possible, incorporate data analysis to increase the effectiveness of your anti-fraud efforts. ■

Conducting Investigation Interviews: Best Practices

By Craig Anderson and Melissa Hall

When interviews are necessary during the course of an investigation, it is always for the same purpose: to find the truth! Depending on the investigation, you may have invested weeks of reviewing data, formulating hypothesis and testing theories to put together the pieces of the puzzle. Now the day has come to interview your subject. As you sit across the table from the subject, look them straight in the eye and ask the hard questions. The truth will reveal itself in many different formats, however, you have to know what to look for. It is imperative during an investigation, as an interviewer, that you use all the tools at your disposal to obtain the facts necessary to draw informed conclusions. One of the best tools available for the auditor is the ability to identify verbal signs of deception.

The truth will reveal itself in many different formats, however, you have to know what to look for.

Verbal indicators of deception often include the following red flags:

- **Discussion of character**
  Consistently referencing their level of integrity: a previous 5 star performance evaluation or extreme loyalty toward the organization. For example, if the subject is going out of their way to ensure that you are convinced that they are a good person and would not consider the types of actions you are investigating.
- **Attacking the process or the person**
  Constantly referring to "flaws" in the process, while not directly answering the questions posed to them. This is a classic attempt to deflect from answering the question and distracting the interviewer from obtaining a clear and direct answer to the questions.
- **Swearing to anyone/anything**
  "I swear to _____!" (Fill in the blank: a deity, a person, on a grave, etc.) is a clear attempt to distract from the question. How dare you even think that their morals would simply allow them to commit such an act?
- **Repeating the questions**
  This is a stall tactic used for the subject to gain enough time to craft a response to the original question. The repetition is usually done verbatim.
- **Use of absolute phrases**
  "I would NEVER, EVER, EVER", "I have NEVER", "Under NO circumstances" are all examples of emphatic language that goes overboard. These should raise the suspicions of the interviewer that the subject is being overly committal to distract from the actual content of the answer.
- **Use of "soft" words**
  If the subject of the interview replaces words in a question to a softer version of the same word, it can indicate that the subject is trying to minimize the seriousness of their actions. For example, use of the word borrow instead of the word steal.
- **Qualifying language**
  "As far as I know" and "to the best of my knowledge" are phrases that make any answer much less direct to the question presented. This may be used to hide their involvement. (It is important to note that these observations do not always indicate guilt, but usually, the behavior does indicate an attempt to hide something, deception, or a topic that the subject doesn't want to discuss. As the interviewer, stumbling across one of these red

ABOUT THE AUTHORS

Craig Anderson *is the Deputy Director, University Audit at Virginia Commonwealth University, where he deals extensively with investigations of fraud, waste, and abuse as well as managing financial and operational audits for the university. He holds a Master of Science degree in Accounting and is a Certified Fraud Examiner.*

Melissa Hall *is the Associate Director of Forensic Audits at the Georgia Institute of Technology, where she deals extensively with investigations of fraud, waste, and abuse in the institute. She is a Certified Public Accountant and a Certified Fraud Examiner.*

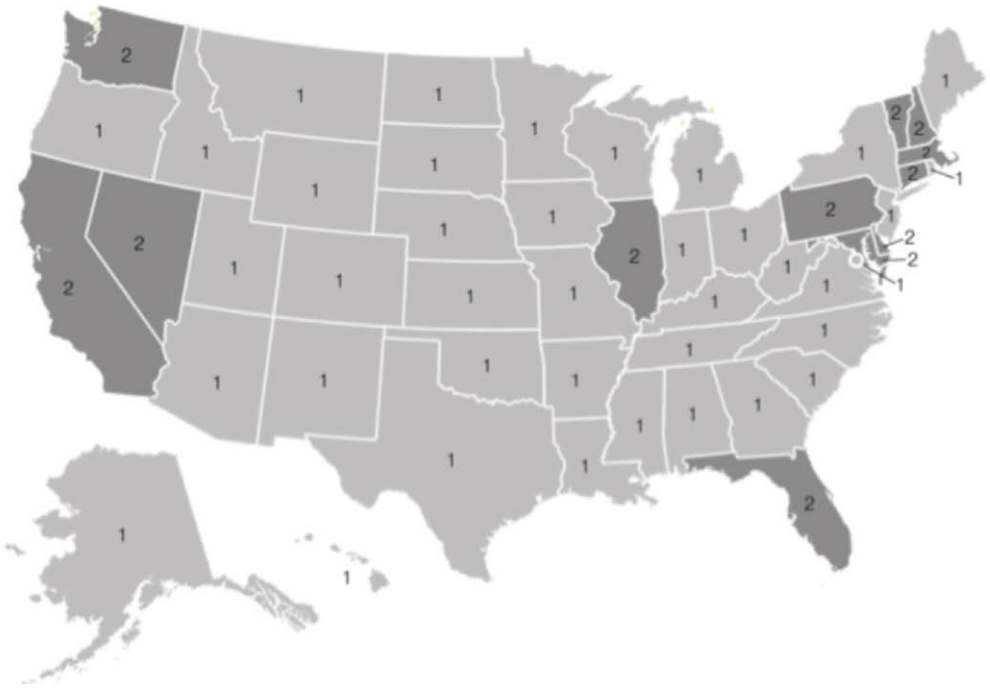
flags, is like finding a needle in a haystack. You should continue with the line of questioning, as it will likely lead to information that you are seeking.

TO RECORD OR NOT TO RECORD

As the interviewer, stumbling across one of these red flags, is like finding a needle in a haystack. You should continue with the line of questioning, as it will likely lead to information that you are seeking.

There are multiple ways to document interviews, but recently, one of the most important questions posed is whether or not to audio record an investigation interview. Digital audio recorders are very inexpensive to purchase, and almost everyone owns a cell phone with audio recording capabilities. But before you decide to audio record your next investigation interview, it is important that you learn the requirements for the state concerning the recording of interview sessions. Some states allow for the audio recording of a conversation as long as one of the participants in the conversation is aware that the conversation is being recorded (1-party state). In the case of a 1-party state, the simple fact that the auditor recording the interview knows that the conversation is being recorded is sufficient not to violate the law. Other states require that all parties involved in the conversation are notified of the recording (2-party state). Therefore, in a 2-party state, if the auditor records the interview without notification to all parties in the interview, the auditor is in violation of the law. In a recent survey conducted of ACUA members, approximately 34 percent of respondents were "unsure" if their state is a 1-party or a 2-party state.

Whether you decide to record or not, know the laws within your state. As of the time of this publication, the states are labeled as 1-party or 2-party states as indicated below:



(Photo courtesy of: http://www.pinow.com/resources/audio-surveillance-laws-by-state)

Based on the results of the recent survey of ACUA membership, it was noted that the majority of ACUA members are not audio recording interviews (75 percent), regardless of whether their state allows for it without disclosure to the parties involved. The survey results indicated that within the ACUA community:

- 5% always audio record interviews
- 20% sometimes audio record interviews
- 75% rarely/never audio record interviews

Never allow an interview to be a one-on-one session as this will lead to a "he said/she said" circumstance if the content is questioned.

The concern around this practice occurs when these survey results are combined with the understanding that 75 percent of the United States allows for audio recording without disclosure, while 75 percent of ACUA members are not currently audio recording interviews.

Whether it is decided to audio record or not, the interviewing methodology must be documented in a defined processes to ensure the integrity of the interview process. Using the information obtained from the recent ACUA survey, along with discussions with auditors in practice, several key pieces of advice can be found as follows:

BEST PRACTICES APPLICABLE TO ALL INTERVIEWS

Here are some best practices that should always be incorporated in an interview, regardless of whether the interview is audio recorded or is documented with handwritten notes.

- Always use two people for the interview process
  - o Never allow an interview to be a one-on-one session as this will lead to a "he said/she said" circumstance if the content is questioned.
  - o One-on-one interviews do not allow for quick adaptation and documentation to be managed effectively.
- Establish an interview lead
  - o One person should be responsible for driving the content and direction of the interview. That is not to say that the second interviewer does not participate but it should be a lesser role.
  - o Second person is mainly responsible for detailing responses to questions posed by the lead interviewer. The second interviewer can also be used to change the "pace" of the interview by injecting a slightly different personality in the process.
- Use of "Pre-prepared" questions
  - o If the decision is made to use questions documented prior to the interview, these documents may be subject to Freedom of Information Act (FOIA) requests.
- Both interviewers should record and identify deceptive actions, both physical and verbal
- Effective use of silence
  - o Over the course of the interview the lead should establish points of time where the interview goes quiet. The uncomfortable nature of quiet will often times get the subject of the interview to "fill" that silence.
  - o Valuable information can often be gleaned from the subject's desire to eliminate the quiet during the interview cycle.

SPECIAL CONSIDERATIONS FOR AUDIO RECORDED INTERVIEWS

Audio recorded interviews provide a convenient way to "revisit" the interview and determine exactly what was said, which eliminates room for errors in recollection. If the decision is made to audio record interviews there are some special circumstances that should be considered to document and protect the integrity of the interview. Some of these considerations include:

Audio recorded interviews provide a convenient way to "revisit" the interview and determine exactly what was said, which eliminates room for errors in recollection.

- In a 1-party state, will the subject be notified that the interview will be recorded? This should be determined prior to the interview.
- How will the audio recording of the interview be secured within the department's workpaper system?
- What policies and procedures have been established to ensure chain of custody and authenticity of the recorded interview?

- What will be done with the auditor's handwritten notes? How should the interviewers create and document a summary of the interview via the use of their notes?
- Will a copy of the audio recorded interview be provided to the subject of the interview?

SPECIAL CONSIDERATIONS FOR NON-AUDIO RECORDED INTERVIEWS

When the decision is made not to use an audio recording device there are many practices that can be put in place to ensure the accuracy and integrity of content of an interview.

Some considerations when not using an audio recording device are:

- Time is of the essence: as quickly as possible the notetaker should ensure that the full content of the interview is put down in writing and reviewed. Once the interview is complete the content of the interview should be documented and reviewed by both parties as quickly as possible.
- Establish a minimum timeline to complete and review the interview write-up. Ideally this would be completed within two to five business days. If the interviewers allow time to go past five business days, it becomes more difficult to ensure exact language is appropriately recorded.
- If it appears that the interview will be a lengthy process, then the lead interviewer should identify a place to take a break. This will allow the interviewers to collaborate and identify any additional areas to cover or to determine potential areas of deceit or concern.
- A department should establish a standard process for conducting and creating a historical record of the interview and the location of the workpapers associated with the interview.

A department should establish a standard process for conducting and creating a historical record of the interview and the location of the workpapers associated with the interview.

As you are developing your internal policies and procedures, other items should also be considered. The use of video recorders to document the interview is completely different than audio recording, as differing laws apply. Video recorded interviews should be coordinated through your legal office to determine appropriateness and allowability. If your state does allow for 1-party audio recording, the subject being interviewed has the same rights to record the interview as you do. Therefore, everyone should assume that the other party is audio recording the interview. ■

Crisis Management: The Calm before the Storm

By Travis Taylor and Judith Islas

Crises are inevitable, and they often hit when least expected. Sound preparation will help your college or university respond as effectively as possible when a crisis lands on your doorstep. Having an effective crisis response plan will help your campus community avoid panic, pitfalls and potential missteps that can result in operational disruptions, negative media attention, harm to your institution's reputation and legal liability.

CRISIS FUNDAMENTALS

Crises on college and university campuses come in all forms. A crisis is any action that threatens your operations, image, services, financial health, community standing, long-term performance or leadership. A crisis can arise from a multitude of events, such as negative social media campaigns, student or faculty protests, violence on campus, financial fiascos and natural disasters. The legal liability resulting from crises can become their own additional crisis. Crises can trigger all types of claims, including negligence, invasion of privacy, breach of contract, discrimination, or any number of alleged statutory or constitutional violations. Crisis readiness can help your college or university avoid certain types of crisis, and in the event of a crisis, an effective readiness plan will help your campus respond and recover as quickly and completely as possible.

The legal liability resulting from crises can become their own additional crisis.

CRISIS READINESS

While the intensity of crises may vary, college administrators can easily find themselves in the "hot zone" when an unexpected event occurs and the media and public assert an immediate need to know what is happening in great detail. Preparing a campus and workplace security plan and a plan for crisis media relations is a critical resource that will help guide administrators through this "hot zone" in a calm, focused, effective way and avoid creating any additional liability.

Federal and state laws require various levels of safety planning and notification in the event of a crisis or hazardous situation.

As a first step to crises readiness, administrators should assess systems and risks specific to each campus to understand what the potential threats are. Risk assessment should be ongoing and used to inform safety and crisis-response planning. In addition to risk assessment and plan preparation, it is essential to provide staff, faculty and students with training and information about the crisis response systems and plans in place.

Federal and state laws require various levels of safety planning and notification in the event of a crisis or hazardous situation. College and university administrators are generally required to have knowledge sufficient to identify hazards; develop safe practices; communicate about potential hazards; communicate about how/who to alert when a crisis occurs (for example, by publishing and posting a safety plan); investigate incidents that occur; work to correct or cure an unsafe condition, incident or problem that could trigger a hazardous incident; record and report incidents that do occur; and provide ongoing safety and communications training to faculty, staff, administrators and students. For example, California's Education Code requires postsecondary educational institutions to prepare, post and distribute campus safety plans. Like the federal Clery Act, California's Education Code also requires postsecondary institutions

ABOUT THE AUTHORS

Travis Taylor, *a Vice President with Fineman PR, is experienced in crisis communications and consults with clients on a variety of communications strategies and services.*

Judith Islas *is Of Counsel in the San Diego office of Liebert Cassidy Whitmore where she counsels clients in all matters pertaining to labor, employment and education law.*

to record and report specified criminal and non-criminal activities that take place on school campuses. Most states also have programs that require initiatives for workplace safety and health, which often align with the goal of providing safe and healthful campuses for students.

When creating a safety plan, several elements are essential: (1) Know who "makes the call." If there is a lockdown on campus, identify in advance the person responsible for making the lockdown decision. (2) Identify emergency contacts and the appropriate law enforcement contacts in your crisis readiness plan. Do not wait until a crisis occurs to figure out whether to call city or campus police. Also, be sure to identify the people who know the emergency contact information. (3) Have a thorough understanding of the notification and alert systems you are using, and that you are required to use, to alert students, faculty, staff and others of a crisis. (4) Finally, assign a person as the college or university's media management contact and identify in advance a high-level spokesperson who will be responsible for credibly addressing the public when a crisis occurs.

Do not wait until a crisis occurs to figure out whether to call city or campus police. Also, be sure to identify the people who know the emergency contact information.

RESPONDING TO A CRISIS

Once you have a plan in place, you will be better prepared to respond when a crisis occurs. When a crisis occurs, the crisis response team should assess the particular threat or incident and contact the appropriate local support agency, as identified in the crisis response plan. A campus representative who can communicate and establish a good working relationship with emergency and medical support personnel throughout the incident – identified in advance – should be appointed to act as a police/emergency personnel liaison. If an individual on campus is causing the threat, engage with emergency personnel to remove the threatening person from campus. In some instances, such a person can have his or her consent to remain on campus withdrawn, can be subject to a temporary restraining order, or, if he/she is a student or employee, can be placed on suspension or leave consistent with college or university policies.

While ensuring that threats are removed, the emergency response team should create a plan of action for the first "48 minutes" and the first "48 hours" following an incident. The team should prepare a communications action plan and message matrix for each audience; review social media and traditional media policies; gather facts to prepare for potential media questions; and adhere to any communication guidelines, flow charts, logs and/or rosters previously prepared for any crisis. The institution's media spokesperson, already identified in the planning process, should handle the relationship with local media, and no other campus personnel should be authorized or permitted to speak with the media without the spokesperson's knowledge and consent. The spokesperson should be an individual who carries credibility – very likely the college president or someone of clearly evident rank and authority.

COMMUNICATING IN A CRISIS

Communicating during a crisis is essential to keeping affected audiences informed. Speaking through the media with a coherent, consistent message about a crisis allows the college or university to tell its side of the story and, if necessary, "set the record straight" rather than allowing others to fill the communication void and shape public opinion consistent with their own perceptions and interests. Coherent, consistent messaging and telling the institution's story first can defuse and even pre-empt criticism, allowing the college or university to shape the message and prevent media or public distortion as the story unfolds.

While it is beneficial to speak with media during a crisis, colleges and universities must also be certain to protect the privacy rights of students and personnel involved in or affected by the crisis. If law enforcement is involved, the college or university's spokesperson should maintain ongoing communication with law enforcement to understand the scope and status of any investigation. The spokesperson must take care not to speculate or admit liability or conduct that supports liability. This may be a particular temptation in the early stages of a crisis when the spokesperson and the crisis team do not yet have all the facts in hand, and initial appearances may prove contrary to the facts that will emerge upon investigation.

Frequently, the underlying events triggering a crisis must be investigated before the facts can be sorted out and determinations of fault and liability assessed. Admitting liability prematurely and without adequate basis is a serious misstep and can unnecessarily and undeservedly create liability. If any

admissions are to be made, that should only occur after all relevant investigations are completed, all determinations are made, and the college's or university's legal counsel, governing board and executive leadership team have all reviewed the investigation and determinations, and agree that an admission is appropriate under the circumstances.

When a crisis is imminent, always do a PANTCHEK:

Public welfare is the first priority.
All bad news out at once.
No blame, no speculation and no repetition of the charges.
Tell your side of the story first and with facts, or take responsibility if you are in the wrong.
Care and concern for affected parties.
High-level spokesperson must be accessible and responsive.
Ensure the problem will not recur, and describe measures taken to ensure this.
Keep separate plan for moving ahead.

When addressing the media, the spokesperson should speak with clear empathy and concern for any affected students or employees and their families. He or she should not panic or rush, should not say "no comment," and should not fail to comment altogether. Rather, the spokesperson should provide all the non-confidential verifiable information available and let members of the media and public know that further reliable information will be provided as soon as it becomes available. All individuals communicating with members of the public or media in a crisis must assume that everything said is "on the record."

MANAGING SOCIAL MEDIA IN A CRISIS

Social media provides ample room for misinformation, inflammatory feedback and the potential to sensationalize or elevate the level of a crisis. Colleges and universities should maintain social media policies that allow them to correct misinformation, demonstrate that they are listening, address genuine concerns, present the school's perspective, and adjust response strategy and messaging as needed. Be sure to maintain consistent messaging across all media platforms and drive inquiries to the main source, such as the institution's website or official social media pages. The more promptly the institution can respond to concerns expressed on social media, the better it will be able to maintain control of messaging.

While maintaining control of social media messaging, also be mindful of the appropriate time to delete content. Note that deleting content is a form of censorship, and must be consistent with the college's or university's social media and communications policies, and corresponding legal principles. Nevertheless, it may well be appropriate or necessary to remove hate speech, personal attacks, threats, spam or speech that violates another person's privacy rights to the extent that such removal is consistent with law and policy.

Finally, the crisis communication team should know when a crisis is over!

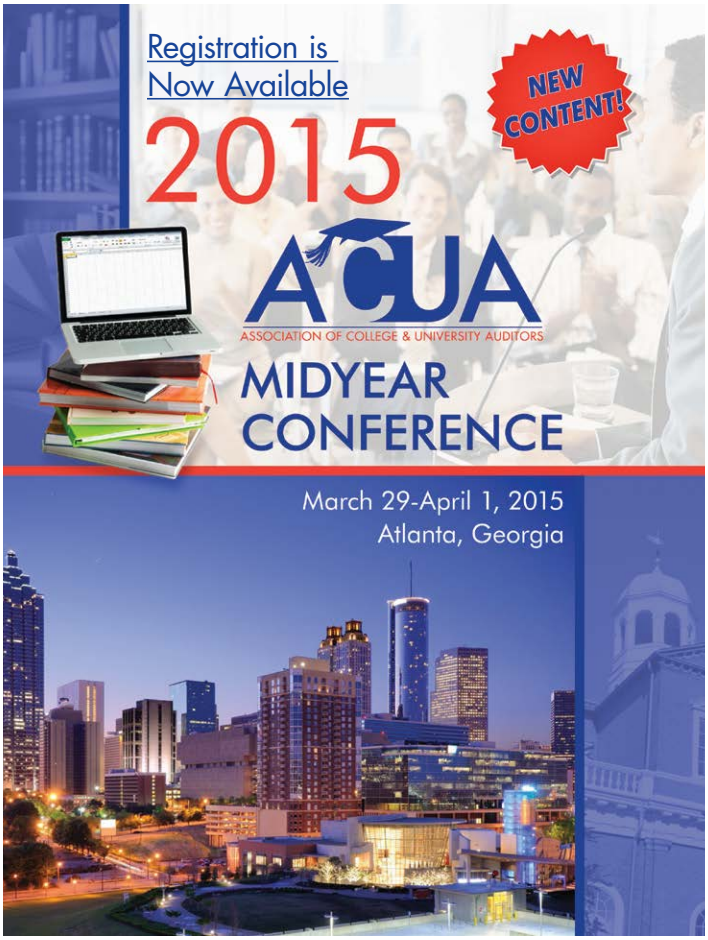
CRISIS FOLLOW-UP

Once a crisis is over, determine what follow-up is legally required or otherwise appropriate and helpful. Federal and state laws may require investigation, due process and hearing opportunities for individuals involved in the crisis. Federal and state laws also may require reporting on the incident to government agencies, and that the incident be included in violence and safety statistics that must be published. State and federal Occupational Safety and Health Standards, the Clery Act and Title IX are all examples of laws that require incident response and reporting. Failure to comply with these legal obligations can result in fines, criminal convictions and private rights of action (i.e., individual lawsuits) against a college or university. In addition to meeting legal response obligations, college and university administrators should follow up after a crisis to assess what went well and what could have been done better in its

response. Finally, following a crisis, the institution should refine its crisis response plan, based on lessons just learned.

KEY POINTS TO REMEMBER

- Prepare a crisis response plan before a crisis occurs, so you have effective guidelines and protocols to follow whenever a crisis hits.
- Develop relationships with media and emergency response personnel. They will be critical when dealing with a crisis.
- Timely responses are critical, but do not panic or rush.
- Facts are not always black and white, and must be communicated, or not, with great care and only when they are definitively confirmed.
- Even when providing definitively confirmed information, be careful not to provide confidential or other private information or information that would interfere with an ongoing investigation.
- Know when the crisis is over.
- Follow-up each crisis by reflecting on and refining the crisis response plan. ■



BEST PRACTICES COMMITTEE OFFERS SURVEY ASSISTANCE

Do you have a few questions that you'd like to benchmark with your ACUA peers? We are available to assist ACUA members in the development of simple (up to 10 questions), ad hoc, online surveys designed to get to the heart of issues and provide high-quality feedback. Please contact Best Practices Committee Member Jon Clark Teglas at jcteglas@vt.edu to discuss your particular needs.

QAR VOLUNTEER RESOURCE LISTING

Are you looking for volunteers to serve on your institution's QAR team? Are you interested in volunteering to serve on a QAR team?

Access the Members Only area of ACUA's website, select "Resources" and "Quality Assurance Review" to review the External Assessment Volunteer Listing database or volunteer. If you have questions, please contact Best Practices Committee Member Lily Reinhart at lreinhart@aa.ufl.edu.