| VOLUME 58 | NUMBER 2 | SUMMER 2016 |

COLLEGE & UNIVERSITY AUDITOR

HIGHER EDUCATION'S SOCIAL MEDIA:

WHO'S MINDING THE STORE?

ACUA
ASSOCIATION OF COLLEGE & UNIVERSITY AUDITORS

INSIDE:

Navigate your evolving challenges through collaboration with Baker Tilly

Modern-day chief audit executives strive to align internal audit (IA) efforts with institutional strategies and help to evolve institutional risk management and compliance. Challenges include staying abreast of the latest regulatory changes, addressing industry hot topics, and accessing the right expertise at the right time. High-performing IA functions leverage Baker Tilly to help their institutions to:

- Understand and address emerging regulations within higher education (e.g., Uniform Guidance, Title IX)
- Augment technical expertise to audit cybersecurity risks
- Develop construction risk management programs
- Address sponsored research compliance and infrastructure effectiveness
- Interface with government auditors (e.g., NSF, NIH) and resolve government audit findings
- Improve institutional operations (e.g., investment management, athletics, advancement, academic integrity)
- Perform value-added quality assessment reviews
- Assess and catalyze institutional efforts to implement enterprise risk management and evolve compliance programs

Connect with us.
bakertilly.com/higher-education

BAKER TILLY

An independent member of Baker Tilly International

Accountants and Advisors

SUMMER 2016
COLLEGE & UNIVERSITY AUDITOR

CONTENTS

FEATURES

SOCIAL MEDIA

FRAUD

COLUMNS

AUDIT TOOLS

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.

Upcoming Deadlines
Fall 2016 Issue – September 1, 2016

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.

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

LETTER FROM

THE EDITOR

By Sam Khan, CISA
Editor

Farewell readers. This is my last edition as editor. It is hard to believe that it has been three years since I began working on the journal as deputy editor and later as the editor. While stepping away from the editor role, I will still be deeply involved with ACUA. I recently took on the newly created role of Communications Committee Chair. In this role, I will be working with volunteers to make the website, journal, social media and ACUA community - the tools we use to communicate and share ideas—work better for you.

In this issue of the journal, we have an article by Emily Kidd called, "Higher Education's Social Media: Who's Minding the Store?" This article identifies the risk of social media in higher education and shows how internal audit can address this rapidly changing area.

ACUA's Best Practices Fraud Subcommittee surveyed ACUA's membership to gather best practices for the prevention of fraud, waste or abuse due to unmanaged or undisclosed conflicts of interest. The article called, "Conflicts of Interest Best Practices: Mitigating Fraud Risk at Your University" offers guidance for addressing this challenge.

Allison MacFarlan has written a follow-up article to her first article, "Know Your Neighbor: The Cloud," which was published in the summer 2015 issue. In part two of her article, she explores the challenges educational institutions face when securing applications and data in the cloud. Her article explores the controls and risks related to federated authentication.

"Auditing Solutions for Higher Education Issues" by Joe Reed and Cathy Miller introduce the idea of repetitive audits which have a narrowly-defined scope of work. These audits focus on a particular part of a process and the same audits are conducted throughout different university units. Performed in a day or less, a draft report is sent to the client within a week.

"Data Analytics: A Management Tool for Addressing Organizational Risks" by Ryan Merryman, Chris Knopik and Matt Anderson explores how data analytics can help build trust. The authors state that when an institution routinely demonstrates accountability, communicates the performance of its programs, and creates transparency, it builds and sustains the public trust.

Volunteering for the journal is a great way to give back to the profession.

"Fraud Education and Awareness: Increasing Employee Fraud Awareness" by Joe Reed and Ralph Kimbrough states that internal auditors cannot be responsible for finding all fraud nor can they be held responsible for preventing fraud. Prevention measures are to be adopted and installed by the administration. Thus, internal audit must find ways to persuade management to adopt methods of preventing fraud and educate management on how to detect fraud when these prevention measures fail.

As always, I encourage your feedback. I am interested in hearing about topics you would like to see in future issues of the journal. Now, as the Communications Committee Chair, I would love to hear your thoughts about how ACUA communicates with you and how we can improve. Please feel free to contact me at (541) 737-7336 or sam.khan@oregonstate.edu. Thank you to all the people who helped make this issue possible. Volunteering for the journal is a great way to give back to the profession. ■

LETTER FROM

THE PRESIDENT

By Vijay Patel CFE, CISA, CPA
President

Greetings ACUA Friends and Colleagues:

Resources! Resources! Resources! The Association of College and University Auditors (ACUA) prides itself on providing quality resources to our members to tap into, which in turn enables them to provide quality service to their respective institutions.

This past April 10-13, 2016, ACUA held its Midyear Conference in beautiful downtown Portland, Oregon. The Midyear Conference is a 2.5-day intensive course in which participants select one of five or more tracks on which to focus. Tracks typically focus on topics such as fraud, compliance, audit essentials, IT or training on audit software.

On September 11-15, 2016 ACUA will hold its 60th annual conference in the heart of Miami where attendees can experience the diverse culture and beautiful beaches Miami has to offer. Annual Conference participants will attend three general sessions, where keynote speakers will present an array of topics, from motivational presentation to fraud experiences. In the past, we have had the pleasure of having keynote speakers such as Cynthia Cooper, CEO, CooperGroup, LLC; Derrick Crawford, Managing Director of Enforcement, NCAA; Bob Kodiz, President, Flight of Ideas, just to name a few. Participants will choose from an array of topics to attend eight breakout sessions during the course of the conference.

Both conferences offer 20 plus CPE credits and participants have the opportunity to join in with networking events, make new friends and catch up with old friends.

ACUA's Risk Dictionary is an invaluable tool, which is available to all our members. Audit shops can access this tool to identify risks and controls, develop audit procedures in the areas they are planning an audit. I have used this tool many times to create audit programs, and it is so easy to use.

ACUA believes that internal auditors add tremendous value to their institutions. To help members promote the overall value and increase awareness of internal audit, ACUA has created a number of resources and made available to our members. Many of the resources can be tailored to meet the needs of individual institutions.

This year ACUA launched its first association-wide mentoring program. Its initial focus being on small audit shops, with the possibility of expanding in the future.

This year ACUA launched its first association-wide mentoring program. Its initial focus being on small audit shops, with the possibility of expanding in the future. Currently, the program has approximately forty participating audit shops.

These are just a few of the many resources available to our members. Almost all of ACUA's resources can be accessed through the website so be sure to explore the site.

Last, of course, none of the above would be even possible without our member volunteers as a resource. So my "CHEERS" and appreciation to the chairs, directors and their supporting volunteers that have spent countless hours and dedication in their respective committees in making ACUA a successful organization. ■

Vijay Patel CFE, CISA, CPA
ACUA President

Higher Education's Social Media: Who's Minding the Store?

By Emily E. Kidd, CIA

There was a buzz on campus regarding a potential change in the mascot. One only had to search on Twitter to see that the hashtag calling for the mascot's removal was trending in the community.

The rumors were flying on Yik Yak. It seemed the professor had indeed gone out with the student the night before, and almost everyone now knew of the impropriety.

The post occurred two minutes after the incident and alerted both students and staff in the surrounding buildings to perform an in-place lockdown. The official account was closely monitored by all to the sounds of sirens for the next two hours. When the all clear finally posted, those on campus met it with relief and gratitude.

The real-time nature of social media and the ubiquitous use of smartphones have us connected to information like never before.

The widespread use of social media at colleges and universities is real. Situations such as these frequently happen as social media platforms often drive information distribution. The real-time nature of social media and the ubiquitous use of smartphones have us connected to information like never before. As governance agents at the institutions we serve, auditors need to be aware of social media and understand its potential impact.

ABOUT THE AUTHOR

Emily E. Kidd *is currently the head of Internal Audit at the City of Reno and is a Certified Internal Auditor with an MBA in Finance & Accounting. Her professional work experience includes internal audit, accounting, and management analysis in multiple industries including state government, higher education, state taxation, and gaming. In addition she is a Board Member for the Institute of Internal Auditor's Northern Nevada Chapter and serves as the chapter's Website Administrator. She is a member of the Institute of Internal Auditors, the Association of Government Accountants, and the Association of Local Government Auditors.*

Background

The new major player in the higher education universe is social media. Social media is understood as the set of web-based broadcast technologies and platforms that enable users to share content and comment on posted material including pictures, videos and the written word. Common current platforms are Twitter, Snapchat, Instagram, YouTube and Tumblr with a multitude of newcomers such as Kik and SoundCloud also becoming important to the students at our institutions. *(Have not heard of those two? At the time of this article, Kik had 1.92 million Android downloads, and SoundCloud had 1.94 million.)*

Cultural Mainstay

We have heard it before, "Our department doesn't need to bother with social media; it's just for the kids." While this statement may have been accepted five years ago, today it is incongruous with reality in our society. For some organizations, a statement such as that can range from being mildly problematic to ignorant to downright dangerous. Because the way people interact with each other and get their information is often rooted in social media, the need to govern the official accounts of colleges and universities is great. And although a higher percentage of millennials use social media than other groups, a significant portion of Gen Xers and, yes, Baby Boomers are participating too. Social media is here to stay, and to ignore it is to play ostrich, with potentially significant adverse consequences.

Social media is here to stay, and to ignore it is to play ostrich, with potentially significant adverse consequences.

Not really convinced? Consider electronic mail. New to most in the mid-90s, it is now so commonplace in personal and business environments alike that we may forget it was not always in use. While most have embraced *this* technology, there has been resistance by some when it comes to social media use. A mindset of "just the kids use social media" is still not uncommon in some organizations. This perception of social media needs to change if we are

to remain relevant in higher education. The adage *change or die* certainly may be applicable as this informational shift continues to change the world around us.

RISKS & GOVERNANCE

These platforms and apps, while fun in their design, have tangible risks associated with them. The very nature of social media is also what makes it risky—real time communication and one-to-many publications.

Legal and Regulatory Compliance

Legal and regulatory compliance presents significant areas of concern when it comes to social media. Among them are the intentional or accidental release of sensitive information, including the possibility of loss of intellectual property; the ability to identify employees using organizational social media to post content with legal ramifications (harassment, etc.); and trademark infringement. Archiving social media data may also need consideration depending on local public records law and disclosure requirements. The regulation of social media use continues to be a gray area for many, leading to uncertainty in policy creation. However, the cost of doing nothing may be high given the risks for the institution. Doing something can do much to avoid or mitigate these risks.

Security and Privacy

Higher education's security concerns have both common and distinctive elements. Securing fiscal information and strategies are common themes across all types of organizations. However, student privacy is essential to us—with the Family Educational Rights and Privacy Act and Health Insurance Portability and Accountability Act in play. Ensuring that these and other matters distinctive to us are considered in the use of social media is vitally important.

Brand and Reputational Damage

Reputational damage is a sensitive and consequential risk in the collegiate environment. Reputation is built slowly over time, and a social media blunder can negatively influence the perception of the institution. Negative perceptions, conscious or subconscious, may impact the choices a potential student makes regarding the institution. If the damage is large enough and its reach broad enough, institutions may see direct losses, such as lost revenue from decreased enrollment.

Reputational damage is a sensitive and consequential risk in the collegiate environment. Reputation is built slowly over time, and a social media blunder can negatively influence the perception of the institution.

A recent EisnerAmper survey of board members found that fewer than four out of ten organizations have a plan to address reputational crisis. The report cautioned, "Public companies should be aware of the connection between a cybersecurity breach, an organization's reputation and the ever-expanding role of social media." Because reputation is such a cornerstone of higher education's business model, the reputational risk associated with the reach of social media needs to be a part of the risk conversation. In the fictional examples at the start of this article, the corresponding risks are reputational, legal and safety.

Governance

Social media governance must be two-fold: management of the official accounts used by the institution and oversight of content. While the second aspect falls into the bailiwick of the communications and marketing department and can be managed with customized metrics, the first aspect clearly points to the need for policies and proper reporting channels. The audit department is an excellent ambassador for establishing such governance in the institution.

MOVING FORWARD WITH SOCIAL MEDIA

Policies

Social media sites and apps are in a constant state of flux, much like the use of social media itself. Due to social media's dynamic nature, creating meaningful policies for it is a challenge. Calling a platform by name in policies necessitates constantly updating policy, which no one wants to do. Imagine having a policy that addresses the password protection of the university's MySpace account, yikes! Instead, using general

terms for social media platforms such as photo sharing apps, video platforms, etc., will keep the organization from needing to update a policy each time a newcomer arrives. Indeed, change is constant. At the time of this article's writing, the phrase *social media* itself has morphed into the quicker 'social' used as a noun—as in, "I searched on social, and he didn't post about the game."

General guidelines for social media account management include who will post, what will be posted, and dual-access. Clear process ownership is central, especially as it relates to crisis management plans. In addition, general recommendations for social media oversight include creating a committee to govern the organization's social media. Other issues to consider include whether there will be acceptance or rejection of public comments; whether the account will interact with users or be a post-only type platform; what the number of posts per day, week or month will be; and whether links to news articles or press releases are allowable.

Strategy

There should not be a lack of transparency regarding how social media is used in an institution. Development of a clear strategy for the use of social media is essential. While the platform may be dynamic, the strategy, as it should be for all functions within a higher education setting, should focus on students and quality education. The mission statement for the institution should drive the strategy for social media use. While different areas of the institution will have various goals for their social media reach, the mission and brand of the institution should be consistent.

Training

Once the policies and strategy have been determined, the training of process owners of official social media accounts must follow. This training should include initial job training as well as consistent, recurring training for staff that manage official accounts. Topics should include policies and procedures, strategy and branding, and crisis management plans.

Audit Plan

Your audit plan's scope will depend on the breadth of your institution's current social media structure. For programs that are in their early stages, the audit may include a review of the governance of social media. Here assistance with policy development may include a gap analysis comparing policies against pertinent laws and regulations. With time, audits would evolve to assess implemented controls that emerged from the initial audit. Later audits may shift to the management of platform access, employee training and compliance. Keeping in mind the institution's current stage in social media development and implementation will always be central when developing the audit plan.

Our audit functions always must adapt to the changing landscape. Including social media in our risk assessments is necessary for us to remain relevant and to help advance and protect our institutions' missions.

Our audit functions always must adapt to the changing landscape. Including social media in our risk assessments is necessary for us to remain relevant and to help advance and protect our institutions' missions. Social media has landed—and is certainly not going away. We need to confirm that our institutions' leaders are engaging with it purposefully. Then on a continuing basis, we need to help assure social media is being used advantageously without assuming unnecessary or inappropriate risks. ■

REFERENCES

Scott, P. R., & Jacka, J. M., (2011). *Auditing Social Media.* Hoboken, New Jersey: John Wiley & Sons, Inc.

The Institute of Internal Auditors, March/April 2015. Reputational Risk, *Tone at the Top Newsletter,* (72).

Breit, M. & Kreit, S. EisnerAmper. *Concerns About Risks Confronting Boards—2015 Survey* January 2016.

Conflicts of Interest Best Practices: Mitigating Fraud Risk at Your University

By Craig A. Anderson, CFE, MS; Melissa B. Hall, CPA, CFE; William A. Hancock, Jr., CPA, CIA, CFE, CISA and Stefanie Powell, CPA, CISA

ABOUT THE AUTHORS

Craig A. Anderson, CFE, MS
Deputy Director
University Audit
Virginia Commonwealth University

Melissa B. Hall, CPA, CFE
Associate Director, Forensic Audits
Georgia Institute of Technology

William A. Hancock, Jr., CPA, CIA, CFE, CISA
Audit Manager
Auburn University

Stefanie Powell, CPA, CISA
Chief Audit Executive
University of North Carolina Wilmington

Consider the following: You are a prominent research faculty member at *Almost Anywhere University.* Your research efforts have just found what you believe is the best invention to solve the world's problems. Your invention could be worth millions of dollars in the open market. You are approached by *Outside Company* to develop this technology. *Outside Company* promptly offers you a contract to make the technology applicable to their products. You accept the contract from *Outside Company* and create *My New Company* for the development and commercialization of the product. *My New Company* develops the technology, and now you need equipment and staff to meet the deliverables with *Outside Company.* You are faced with investing hundreds of thousands of dollars for equipment and hiring staff to work on your technology development, or assuming no one will notice, using *Almost Anywhere University's* lab and students as labor to fulfill *My New Company's* contracts with *Outside Company.* You view it as incidental use of the equipment, noting that the students are receiving a top-notch education and real-world experience. Therefore, there is no need to get approval, compensate the students or contact the University to rent the space and equipment. However, prosecutors view it differently. You have just committed fraud.

A conflict of interest (COI) arises when an employee involved in multiple activities may not be able to separate the conduct of these activities due to financial, familial, or other interest of the individual. These situations can exist in fact or appearance. In either case, a conflict can present problems to the individual and the organization. The risk of COI is inherent in the higher education environment, where faculty and staff are encouraged, rewarded, and promoted for collaborating, consulting, bringing in donors, and conducting the most cutting edge research, all while they educate tomorrow's leaders. In other words, the risk of fraud or misappropriated resources is a tangible and recurring reality in higher education, and the lines of right and wrong can sometimes be blurred. Our universities' leadership looks to internal auditors to help ensure internal controls aid in detecting fraud by reviewing procedures intended to deter and prevent it. **So how do we assist in preventing the issue above from *Almost Anywhere University* from happening on our campus?**

A conflict of interest (COI) arises when an employee involved in multiple activities may not be able to separate the conduct of these activities due to financial, familial, or other interest of the individual.

ACUA's Best Practices Fraud subcommittee surveyed ACUA's membership to gather best practices for the prevention of fraud, waste or abuse due to unmanaged or undisclosed COI and offer the following guidance:

1. Have all employees disclosed potential conflicts of interest at least annually with implemented penalties for noncompliance?

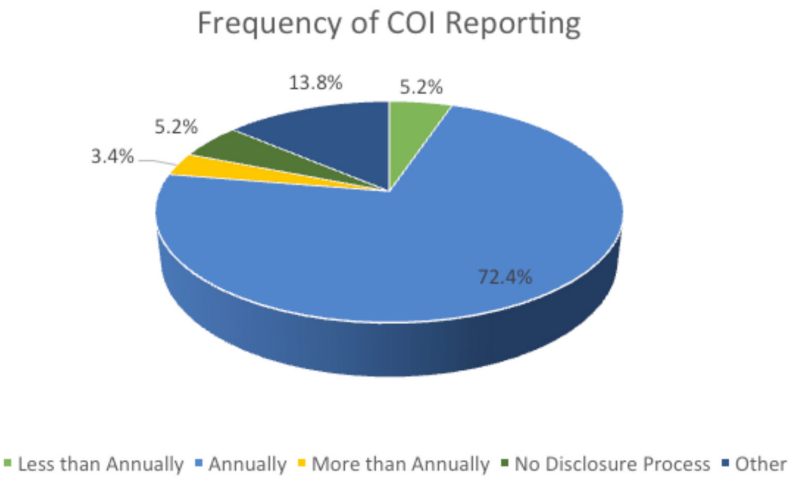
Many of the universities responding indicated that all employees are required to disclose potential conflicts of interest at least annually. Additionally, the guidance for employees often included a requirement to update their disclosure throughout the year if circumstances

changed. Seventy-two percent of ACUA's survey respondents required annual disclosure of potential conflicts, while 5% of respondents did not have any disclosure process. ***(Figure 1)***

If your university is opposed to making ALL employees complete the disclosure, consider that among ACUA's membership, employees in "positions of trust" (such as within Procurement, Research, Finance, Internal Audit, and the Board) are typically required to disclose, even if not all employees are.

However, the best plans for requiring disclosure can be thwarted if the disclosure process is not monitored or if there are no penalties for noncompliance. Fifty-eight percent of ACUA's survey respondents did not have a penalty for nondisclosure. Those that did had varying degrees of penalties, including not being allowed to submit further research proposals and other disciplinary actions up to termination of employment. **If your university is requesting that each employee complete a disclosure, but no one is monitoring the disclosures, then some may ask, "Why complete the disclosure?"**

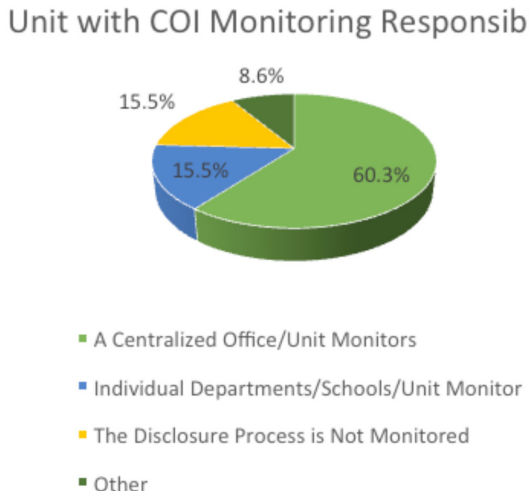
Figure 1: Conflicts of Interest Management *(As reported by ACUA members, Spring 2016)*



2. Consider implementing an automated conflict of interest disclosure process with centralized monitoring

An automated process in our decentralized environments might assist management in ensuring compliance. Automated processes increase efficiency, compliance, monitoring and transparency. Sixty percent of the respondents had a central office that monitored the disclosure process to ensure compliance. Research, Human Resources, Compliance, the Provost's Office, and Procurement were the most common units cited as monitoring completed disclosures. An additional 15% of respondents did monitoring at the unit level. ***(Figure 2)*** **If your university makes the process too complicated and hard to complete, then will your employees comply?**

Figure 2: Conflicts of Interest Management *(As reported by ACUA members, Spring 2016)*



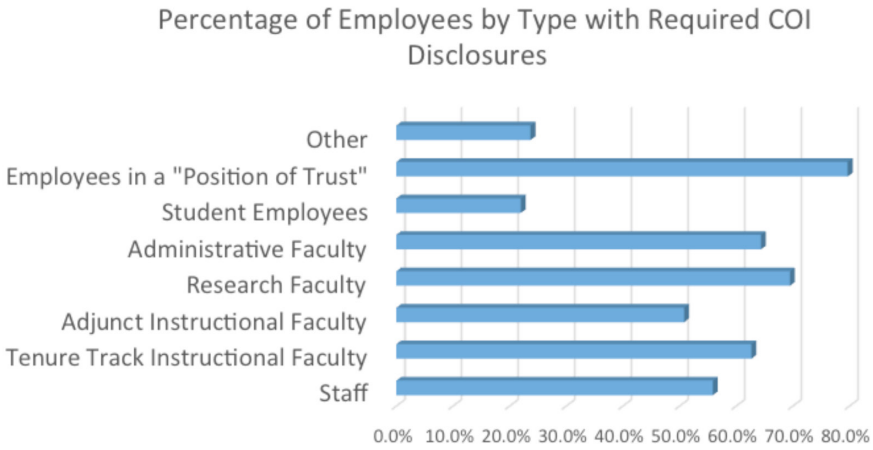
3. Require a written plan for oversight and management of the disclosed conflict

Once a potential COI gets disclosed, best practice includes having a written conflict management plan. Fifty-six percent of respondents indicated that their university required a written plan for management of disclosed conflicts. Such plans were variously managed, sometimes by the supervisor, school chair, Purchasing, or a COI office. Although the majority of the respondents indicated that oversight of the plan was handled at the departmental level, it is a best practice to notify a unit outside of the affected unit, such as Procurement, Internal Audit, General Counsel or Compliance (including Research Compliance). **If your university does not require a written management plan, then how can it ensure the conflict is managed appropriately?**

4. Create a dedicated conflict of interest committee or comparable oversight body

Seventy-four percent of respondents in the survey indicated that their university did **NOT** have a dedicated COI Committee or comparable oversight committee. Management of disclosed conflicts at those universities was handled internally at the departmental level, most often without required notification to any external group. Our review found it is best practice for an outside entity to review and monitor the conflict management plan. This required notification can assist in creating transparency in the process. **If your university does not have an oversight body for the COI process, how can it be sure that departments are managing conflicts appropriately?**

Figure 3: Conflicts of Interest Management *(As reported by ACUA members, Spring 2016)*



Executive leadership relies on internal auditors, as trusted advisors, to recommend changes to current processes and to assist in mitigating risk. Often knowledge of what works on other campuses can be used to assist in educating leadership. The majority of respondents in the survey indicated that their campus had not had a "major fraud, waste, or abuse due to an unmanaged or undisclosed conflict of interest." Although the statistics suggest the risk may be lower than expected, the details disclosed by respondents who indicated their campus had a significant incident showed the risk of loss was much higher when the appropriate controls were not implemented around COI. The majority of respondents indicated that they could not discuss the details of their fraud cases due to ongoing criminal investigations. Each university must also consider the reputational and regulatory risk that is inherent when a real or perceived conflict is identified. If the conflict is documented and managed, management has a level of protection, having done due diligence in identifying and managing COI risk. **Considering the impact of criminal investigations associated with unmanaged or undisclosed conflicts of interest, the question might be asked, "How many can your university handle?"** ■

ACUA's Best Practices Committee would like to thank all the participating universities for their responses to the survey.

Fraud Education and Awareness: Increasing Employee Fraud Awareness

By Joseph Reed, CIA, CFE and Ralph Kimbrough, CPA, CIA

Have you ever completed an audit only to find later that a fraud had been uncovered that you did not find? What is the administration's first reaction? The most common reaction is "Why did you not find the fraud?" or "Did you do a thorough enough job to find fraud?" No auditor, whether external or internal wants to be in that position. Fraud, of course, can be discovered in areas not touched by internal audit. Regardless, the accusations remain: "Internal Audit is not protecting the organization adequately" or "Internal Audit failed to see the risks of fraud before they occurred." Rightly or wrongly, management tends to look to internal audit as the solution to both detecting and preventing fraud. However, as we see in this article, internal auditors cannot be responsible for finding all fraud nor can they be held responsible for preventing fraud.

INTERNAL AUDIT RESPONSIBILITIES

Internal Audit's activities vary by institution. Some concentrate on consulting, others perform operational audits, and still others emphasize financial audits. Regardless, of the primary function of an internal audit department, internal auditors can advise on policy and procedures and make recommendations that would help to prevent fraud. However, to maintain independence, internal auditing is not in a position to force the adoption of additional policies or procedures to discourage fraud. Prevention measures must be adopted and installed by the administration. Thus, internal audit must find ways to persuade management to adopt methods of preventing fraud and educate management on how to detect fraud when these prevention measures fail.

Thus, internal audit must find ways to persuade management to adopt methods of preventing fraud and educate management on how to detect fraud when these prevention measures fail.

PROTECTING THE INSTITUTION

The University of Kentucky (UK) has a program that discourages fraud and creates an atmosphere that increases fraud detection and prevention. The foundation of this program includes the existence of UK's Code of Conduct, annual fraud training, proactive activities such as announced audits and incident reporting. For this program to work well, a team of administrators must work with and support the University of Kentucky's Internal Audit Department (UKIA) on a continuing basis. This support team includes public relations, top administrators, UK Legal, and UK's Police Department. These factors work together to create a structure that provides fraud awareness, promotes fraud prevention and concludes with the outcomes that follow the completion of fraud investigations. The creation of this fraud program has enhanced UKIA's image on campus. In so doing, UKIA has gained ownership of most fraud investigations at the University of Kentucky.

HOW UKIA OBTAINED OWNERSHIP OF FRAUD INVESTIGATIONS

So how did this all come about? It took discipline and perseverance from the audit staff to get UKIA to this point. First, UKIA developed training programs in 2006 to encourage fraud awareness. This training included cash handling and purchasing card processing. Fraud awareness training was introduced in 2007. In 2013 this fraud awareness training was adopted into a fraud program titled "The Business of Fraud." This seminar discussed topics such as fraud definitions and indicators. Tips on fraud detection and fraud prevention were also discussed.

ABOUT THE AUTHORS

Joseph Reed, CIA, CFE
Internal Audit Senior Director, University of Kentucky

***Joe Reed** joined UK's Internal Audit staff in March 2004. He has a Mechanical Engineering degree and an MBA from the University of New Haven. His professional experience includes Finance, Project Management and Operational Management. Previous work experience includes owning and operating a restaurant franchise with his spouse, as well as facilitating operational and financial workshops.*

Ralph Kimbrough, CPA, CIA
Audit Manager, University of Kentucky

***Ralph Kimbrough** joined UK's Internal Audit staff in May 2012. Ralph is a CPA and CIA and he holds a Ph.D. in Higher Education Administration. Ralph's previous work experience includes public accounting, private accounting, internal auditing and teaching. He has managed the internal audit function at other universities.*

This signature fraud seminar is performed eight to nine times annually. The course is required if staff members want to obtain certification for business operations.

Next, measures for fraud detection were adopted by UKIA. This includes providing fraud tips, which UKIA has received from employees, students, audit activities, hot line notifications and administrators. One should not underestimate the potential of receiving tips from multiple sources. Many frauds are discovered by fellow employees who provide tips to management.

Fraud prevention is further enhanced by unannounced or surprise audits. By performing surprise audits, UK staff members are alerted to the fact that UKIA is continually checking for potential thefts or frauds. It is through collaboration with UK Legal, UK Police, Information Technology, and the administration that fraud detection has become a major factor in finding fraud.

In conclusion, UKIA has created a program that encourages fraud awareness and assists in the detection of fraud through functional activities such as training, committee participation and auditing.

FRAUD INVESTIGATION OUTCOMES

Finally, when UKIA is performing the investigation, the outcomes of the investigation are represented by the administration's actions to prevent further occurrences of fraud. UKIA plays an integral part in advising the administration on how to implement measures that will reduce the chance of fraud recurrences. Such measures as changes in UK policies or procedures, improved supervisory training and more emphasis on employee responsibilities are just some of the ways fraud can be discouraged.

In conclusion, UKIA has created a program that encourages fraud awareness and assists in the detection of fraud through functional activities such as training, committee participation and auditing. Additional seminars are currently being considered to further communicate red flags and risk to the university. The importance of communication is constantly reinforced by UKIA at committee meetings and communication outlets. With a program of fraud awareness and management communication, UKIA can set the tone that discourages and detects fraud. ■

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@kellencompany.com, call 913.222.8663 or visit the ACUA Store on ACUA's website www.acua.org for more information.

Know Your Neighbor, Part 2: Cloud Providers and Security

By Allison MacFarlan, CISSP, CISA

Editor's Note: *This is a follow up article to, Know Your Neighbor, Part 1: The Cloud, which was published in the summer 2015 issue.*

As more information technology (IT) services move to the cloud, educational institutions are faced with the challenge of securing applications and data stored in the cloud. Many institutions have implemented federated authentication for permitting access to data and applications. This article will review the controls and risks related to federated authentication.

As more information technology (IT) services move to the cloud, educational institutions are faced with the challenge of securing applications and data stored in the cloud.

Federated authentication holds the promise of reduced IT cost in the cloud becomes a reality. However, overconfidence in our interactions with the cloud application may be misplaced if there are problems with our local identity controls, which can be amplified when services are transitioned to the cloud.

The convenience of having a web application accessible from anywhere has increased our reliance on third-party providers to maintain secure web forms, enforce secure authentication, and distinguish correctly between the identities we present to them, including the entitlements of user roles.

The important elements in an identity exchange with a cloud provider are the identity principals, their entitlements (roles), authorization and access, which should be protected by encryption in transit. Local governance of identity management should ensure that the principle of least privilege is applied to user entitlements and that updates to user identities and roles are done in real-time. If identities are not deprovisioned in a timely fashion or roles are not monitored for changes in job function, then what you send to the cloud service could provide an opening for the public hacker.

Most cloud providers support SAML (Security Assertion Markup Language), the open source, XML-based (Extensible Markup Language-based) assertion framework that enables your institution to deliver information about identities and entitlements in a standardized and hopefully safe way. SAML can interact with ADFS, Microsoft's Active Directory Federation Service; it can also use Shibboleth, the middleware (sponsored by Internet2) that "speaks" to the web's CAS (Central Authentication Service) or to Pubcookie, if that is your local primary authentication service. Some institutions are also using OpenID, another open source standard for cooperating providers, and its related access service, OAuth. OAuth is distinct from the other three because it is just a framework for allowing a user who is authenticated to an OpenID provider (like Facebook or Google) to access some data that your institution controls without having to prove his or her identity to your institution. As the Wikipedia page indicates, OAuth *facilitates* access with a pseudo-authentication,[1] but you have no idea what is behind the ID. Google and Twitter users, even if they are completely anonymous, can be permitted to access resources your institution controls, if someone has authorized their e-mail addresses.

All three of the primary authentication protocols (ADFS, SAML, and OpenID) are designed to be flexible, and as such, they do not have much inherent security. While SAML enables the *exchange* of security and identity information, it does not perform the authentication. The authentication still happens locally, and that token, in the form of an XML string, is passed to the cloud service and also abstracted as it moves into the service and back. The three entities exchanging this token are your organization, which is the Identity Provider (IdP); the identity

ABOUT THE AUTHOR

Allison MacFarlan *is the Information Security Officer at Radford University.*

[1] https://en.wikipedia.org/wiki/OpenID#OpenID_vs._pseudo-authentication_using_OAuth

Columns

Service Provider (SP), which is the Federator (often InCommon[2] for universities); and the Relying Party, the cloud provider.

When identity information is exchanged between the IdP and the SP, the SP (Federator) does not know whether the assertion has been intercepted by another party, whether the user's identity has been hacked, or whether the IdP/university has a secure login form. Authentication tokens are also subject to several attacks if they are not secured with timing controls and encryption. One such attack is a replay attack, where the token is used again by someone else; an HTTP (Hypertext Transfer Protocol) referrer attack, where the client browser gives incorrect information about where it has just been. Another example is an injection attack, where the token is manipulated by another party. These kinds of attacks could be the subject of an entire article. What is important to recognize is that a lot can go wrong in this web-based exchange even before you start putting data into the cloud.

In federated authentication environments, certificates are a must, both for the authentication activities themselves and for the API (application program interface) communications within the application. The APIs do all the hard work in cloud environments: they translate software requests, they manage web communication, they carry authorization keys, and they make the calls to the cloud provider's service. When the customer sends a request to the web address of a cloud interface, the API should always use the customer's X.509 key—this is known as key pinning.[3] If the key is not pinned to the customer certificate, a hacker can execute a man-in-the-middle attack by intercepting a call to the cloud application with another certificate. The SAML framework supports pseudonyms and other one-time identifiers to grant access to other integrated applications, and these should be digitally signed. Otherwise, that abstraction can be exploited later on.

You might be tempted to forego federated authentication entirely, but then you are faced with how to exchange identity information. One very basic method of provisioning access between your institution and a cloud service provider is to use LDAP (Lightweight Directory Access Protocol) synchronization. However, this kind of identity exchange is not good for at least two reasons: 1) if your institution has a termination in between LDAP updates to the cloud service, the user could alter data, depending on his or her level of access, and 2) it is hard to do this without synchronizing the entire LDAP store. Since most services do not require the upload of the entire LDAP database, you would be exposing more identity information than necessary. Inadequate identity cleanup can also cause a user ID to persist on a cloud service long past termination. For LDAP synchronization, there should also be security controls around the daily file synchronization routine (encryption, signing, hashing). Employing a federated identity service is better because your institution controls the identity, the status, and what is needed by the cloud provider (usually an ACK (acknowledgment)) to gain access to the cloud application.

Once your institution develops the appropriate controls and governance around federated authentication, then the promise of reduced IT cost in the cloud becomes a reality.

In a university, there may be people you have to authorize who are not members of your community: parents, guardians, even some auditors. In this instance, you might enable the OAuth framework, which relies on Facebook or Google to authenticate the user, and your institution would thus give these "strangers" access to certain information on a web form. When you use OAuth for this purpose, like providing parental access to tuition or grades if authorized, you will have to build strong local policies and procedures around the likelihood that those users will have their passwords hacked. How would you detect the misuse of a parent's account, and what would you do to prevent the hacker ID from getting to the URL (Uniform Resource Locator)? Logging is essential in this context because you have to monitor privileged access from an identity you do not control. Make sure that you have a way to easily terminate an OAuth ID in an application, from both a procedural and an application standpoint.

Once your institution develops the appropriate controls and governance around federated authentication, then the promise of reduced IT cost in the cloud becomes a reality. This transfer requires work—both for the local IT staff managing identity and integration and for compliance, which has to verify that the service provider adheres to standards that enable the secure transfer and storage of information.[4] ■

[2] https://www.incommon.org/federation/metadata.html

[3] https://www.owasp.org/index.php/Pinning_Cheat_Sheet

[4] Some of these elements are provided in the Statement on Standards for Attestation Engagements (SSAE) 16, Service Organization Controls (SOC) 2, Type 2 report.

IDEA
Data Analysis Software

Unlock the power within your data.

Discover
the secrets hidden in your data

Visualize
your data graphically within dashboards built by you

Advise
your business based on better insights

As an ACUA Strategic Partner, we help college and university auditors:

- Prevent fraud schemes including P-card misuse, false vendors and fraudulent reporting
- Analyze student records to compare disbursed amounts for each federal program
- Analyze federal student aid regulations to identify non-compliance

Exclusive Benefits for ACUA Members

- Preferred pricing on IDEA, IDEA Server and all Audimated Apps
- Discounts on annual license renewals
- Discounts on IDEA training events
- Special sessions at ACUA Midyear and Annual Conference

Interested in IDEA? Contact us at **888.641.2800 / info@audimation.com** for a live on-line demonstration. Visit **audimation.com** for free webcasts and videos, training opportunities, and other helpful content.

Data Analytics: A Management Tool for Addressing Organizational Risks

By Ryan Merryman, CPA, CFF, CITP, CFE; Chris Knopik CPA, CFE and Matt Anderson CPA, CFF, CFE, ASA

An educational system must maintain the trust of its stakeholders to fulfill its mission. Demonstrating accountability is an effective means to build trust. A powerful and cost-effective management tool that helps enhance accountability is data analytics. Data analytics can help identify fraud risk, improve process efficiencies and assist in decision making.

Governments, businesses, nonprofit organizations, and individuals generate, collect, and store an incredible volume of data. Most organizational information is translated into a digital form. Higher education institutions do this with an immense variety of data, from financial transactions to program results, demographics, student profiles, loan applications, scholarships, grants, and more.

A powerful and cost-effective management tool that helps enhance accountability is data analytics. Data analytics can help identify fraud risk, improve process efficiencies and assist in decision making.

The stored data represents the comprehensive documentation of activities and a possible treasure trove of insight into institutional performance. Data analytics can provide enhanced accountability, improved performance reporting, and greater transparency—all producing greater trust in institutional performance.

The goal is to focus efforts on the greatest risks. This can be done using data analysis tools that can evaluate virtually any financial and nonfinancial data and analyze 100 percent of a data population. The procedures can identify high-risk transactions and will often uncover additional areas that may be of concern.

IMPROVING ACCOUNTABILITY

So, what can an institution do with its data that will improve accountability? The first thing is to ensure that funds are being spent appropriately, and assets are safeguarded. By establishing a capacity to perform data analytics, institutions can proactively address the risks present in a variety of transaction types and data sets.

STRENGTHENING INTERNAL CONTROLS

Identified weakness and exposures can then be addressed through strengthened policies and internal controls. Once weaknesses have been addressed and resolved, the level of internal control required by senior executives will be more strongly supported and documented. Also, it is possible that measurable savings from reduced or eliminated fraud and abuse can be reported. Finally, by inserting data analytics methodologies into monthly transaction cycles, management can benefit from the confidence that risks are being mitigated on an interim basis, and not just on an annual basis.

Case Study One—Loan Default Risk: A higher education institution that provides student loans to borrowers at fixed rates wanted to understand the risks that made up their loan portfolio and transactions. After applying data analytics, the institution was able to understand which individuals with outstanding loans had a material difference from one year to the next. Data analytics also uncovered the individuals who had the most loans outstanding. These two pieces of analysis show the institution where to look for loan default risk.

ABOUT THE AUTHORS

Ryan Merryman, CPA, CFF, CITP, CFE
Senior Manager
CliftonLarsonAllen

Matt Anderson CPA, CFF, CFE, ASA
Principal
CliftonLarsonAllen

Chris Knopik CPA, CFE
Principal
CliftonLarsonAllen

ELIMINATING RISK AND BUILDING CAPACITY

Utilizing data analytics to eliminate risk can also build a capacity to conduct enhanced financial analyses. This can lead to improved financial management performance in such areas as cash management, asset management, revenue forecasting, purchasing efficiency, human resources planning and management, and management of deferred maintenance. A very important benefit of data analytics is the ability to plot trends for an extended number of years, not just for the two years covered in an annual financial report.

Improving performance reporting through the use of data analytics will permit institutions to mix and match a variety of statistics and tailor reporting to segments of stakeholders. This improved reporting will also strengthen the content of traditional performance reporting.

Case Study Two—Disbursement Overages: A state college system with more than 30 campuses wanted to understand the risks related to its payroll and non-payroll disbursements. Data analysis revealed that faculty and staff were being compensated above their approved assignments.

HOW TO GET STARTED IN BUILDING A CAPACITY FOR DATA ANALYTICS

One convenient way of exploring and testing the use of data analytics is to initially focus on applying it to financial transactions. Selected external auditors currently utilize data analytics during the course of their financial statement examinations and can provide guidance on software selection, staff training, computing capacity, project coordination and evaluation of results.

When an institution routinely demonstrates accountability, communicates the performance of its programs, and creates transparency, it builds and sustains the public trust.

Once an initial staff capability is established, data analytics can help build financial analysis capabilities and reporting performance. For institutions just getting started, a publication of the American Institute of Certified Public Accountants (AICPA), Computer Forensic Services and the CPA Practitioner, will also be helpful.

HOW DATA ANALYTICS CAN HELP BUILD TRUST

When an institution routinely demonstrates accountability, communicates the performance of its programs, and creates transparency, it builds and sustains the public trust. Data analytics can help build and sustain that essential trust. ■

Auditing Solutions for Higher Education Issues

By Joseph Reed, CIA, CFE and Catherine Miller, CPA

To arrive at appropriate auditing solutions, we must first understand the current problems and issues that exist in higher education. The focus of this article is to discuss higher education culture and appropriate auditing solutions. The auditing solutions are derived from our experiences over the past several years. These solutions may differ based on the specific culture of the institution.

HIGHER EDUCATION OVERVIEW

Higher education is an industry and environment unlike any other with factors such as students, faculty, academic freedom and agreement by consensus. Common Issues arise as a result of this environment, and consequently so does the associated risks or barriers. To address the risks, we must arrive at appropriate auditing solutions. These solutions affect needed change in the culture—we have then come full circle.

The focus of this article is to discuss higher education culture and appropriate auditing solutions.

We considered seven higher education cultural elements with respective common issues and risks as follows. Keep in mind that this list is not exhaustive.

Leadership in higher education is very different from other industries in that it is comprised of a majority of faculty. A common issue that arises is the training provided to faculty to lead the University. In most cases, training is sorely lacking or nonexistent. The resulting risk is a lack of business acumen on the part of University Leadership.

Tenure is a phenomenon of the higher education culture. A common issue with tenure is competency. Once tenure is achieved, the faculty may be less motivated to stay abreast of his or her field of interest. As a result, there is a risk of substandard instruction or research.

The decentralized environment is a part of the higher education culture. Departments operate as silos, disconnected from each other. Therefore, a common issue is standardization. Each unit has its way of doing things, resulting in the risks of inefficiency and ineffectiveness.

Ownership in higher education resides with those departments that "own a process" (e.g. payroll, accounts payable) that occurs in every unit throughout the entire university. A common issue is authority. While the owner is responsible for compliance, authority rests at the unit level. As a result, appropriate compliance with regulations may not be achieved at the unit level.

Students are the overarching reason higher education institutions exist. A common issue that surrounds students is the "adolescence" phenomenon. As a result of their adolescent behavior, students may find themselves failing and dropping out. The risk is a reduction in the very revenue that, in large part, keeps the university afloat.

Gifts are the lifeblood of our academic institutions. Many gifts are given as part of a multi-year campaign. A common issue is the accounts receivable associated with these campaigns which often fund major initiatives. The resulting risk is the lack of needed revenue should the pledged gifts become uncollectible.

Business continuity is of utmost importance to our higher education institutions. A common

ABOUT THE AUTHORS

Joseph Reed, CIA, CFE
Internal Audit Senior Director, University of Kentucky

***Joe Reed** joined UK's Internal Audit staff in March 2004. He has a Mechanical Engineering degree and an MBA from the University of New Haven. His professional experience includes Finance, Project Management and Operational Management. Previous work experience includes owning and operating a restaurant franchise with his spouse, as well as facilitating operational and financial workshops.*

Catherine Miller, CPA
Audit Internal Manger, University of Kentucky

***Catherine Miller** joined UK's Internal Audit staff in July 2008. She has professional experience in Accounting and Business Administration. She has a University of Kentucky bachelor's degree in Accounting as well as a CPA professional certification.*

issue is the funding needed to develop appropriate business continuity plans. As a result, the risk of a major business disruption exists.

ISSUE IDENTIFICATION

Issue identification is about doing risk-based auditing, i.e. "doing the right work." As a result, relevant issues are addressed by constructing action plans to confirm and resolve outstanding problems, prepare for emerging risks, reduce obstacles and ultimately add value to the institution by providing astute findings and appropriate recommendations.

AUDITING SOLUTIONS

We utilize the following auditing solutions at the University of Kentucky to address the issues identified as discussed in the previous section: division trending, repetitive audits and communication methods. Each of these solutions will be explained below.

Trending by division-appropriate solutions demands ample coverage of the entire university. Therefore, we divide UK into six enterprise divisions and record division trends as we perform our work:

- Academics: report to the provost e.g. College of Agriculture
- Administration: report to the president e.g. Athletics
- Affiliates: separate corporations over which UK exercises effective control
- Campus Operations: non-academic units that report to the Provost e.g. Student Admission and Registration
- Finance and Administration: report to the executive vice-president for Finance and Administration e.g. Human Resources
- HealthCare: report to the executive vice-president for Health Affairs e.g. Chandler Emergency Department

REPETITIVE AUDITS

The attributes are described below to serve as an introduction to repetitive audits (RA).

The RA involves evaluation of unit practices related to a process that is performed across the entire university (e.g. procurement card). The RA has a narrowly-defined scope of work. The audit focus may be on a particular part of a process. The RA emphasis is on regulatory adherence. The following question is answered by the RA: Do unit practices comply with regulations governing the process? UKIA conducts the same audit in different university units. The RA is unannounced. It is performed in a day or less with a report draft to the client within a week. UKIA receives a lot of "bang for the buck" with the RA as it serves as a window to a unit that is new to UKIA.

WHY ARE RAS PERFORMED?

- To evaluate adherence to applicable federal, state and university regulations
- To provide audit coverage across the entire university
- To trend audit results within each enterprise division and across the university.
- To serve as a fraud deterrent by identifying red flags during the RA and also increasing the perception of fraud detection via the unannounced or "surprise" element.

The RA results are summarized in chart form on the first page of the report with partially and not satisfactory results explained in the subsequent pages of the report.

The types of RAs are limitless. In addition to procurement cards, UKIA either performs or has in the development stage the following:

- Nonexempt Overtime Compensation (FLSA)
- FERPA

- Cash Handling
- Grant Adherence
- Travel
- PCI-DSS

Communication methods include collaborating with process owners to provide client assistance, policy revisions and process enhancements. UKIA also has general communication including our tip of the month on our website and we conduct various workshops including *The Business of Fraud and Account Reconciliations.*

CONCLUSION

UKIA incorporates the above auditing solutions in our annual audit work plan. We divide our work plan into the following five sections:

- Compliance Program: Regulatory Risk and Audit Coverage
- Business/Operations Audits: Financial and Operational Risk
- Information Technology Audits: Information Security and Data Integrity
- UKIA Infrastructure Plans: Continuous Improvement
- Unplanned Activities: Consultations, Inquiries/Investigations, Red Flags

These solutions continue to be improved and refined over time as UKIA strives to be an audit function that continuously improves and adds value to our institution.

Execution of the above auditing solutions within our work plan has proven to be both challenging and rewarding. These solutions continue to be improved and refined over time as UKIA strives to be an audit function that continuously improves and adds value to our institution. ■

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.

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.

Quality Assessment Review (QAR) Report Comment Repository

Facilitated by the ACUA Best Practices Committee

In Development Now

QAR report comment repository (including recommendations and best practices):

- Identification of relevant issues.
- Proactive preparation for your next external QAR.
- Compilation and analysis of aggregate data to provide useful statistics on common problem areas.

Help Us Help You

Consider sharing your QAR report. The more reports in the repository, the more useful the tool will be! Only generic information will be included (institutions will not be identified).

Submit Your Report

1. Login to www.ACUA.org.
2. Navigate to the Resources tab > Audit Tools > Quality Assurance Review.
3. Follow the Web page instructions for submitting your QAR report.

REGISTER TODAY

ACUA
ASSOCIATION OF COLLEGE & UNIVERSITY AUDITORS

2016 ACUA ANNUAL CONFERENCE

September 11-15, 2016 InterContinental Miami Miami, FL

Members

Wolters Kluwer

When you have to be right

TeamMate® Analytics

Effective data analytics is simpler and more affordable than you think.

Learn more:

TeamMateSolutions.com/Simple