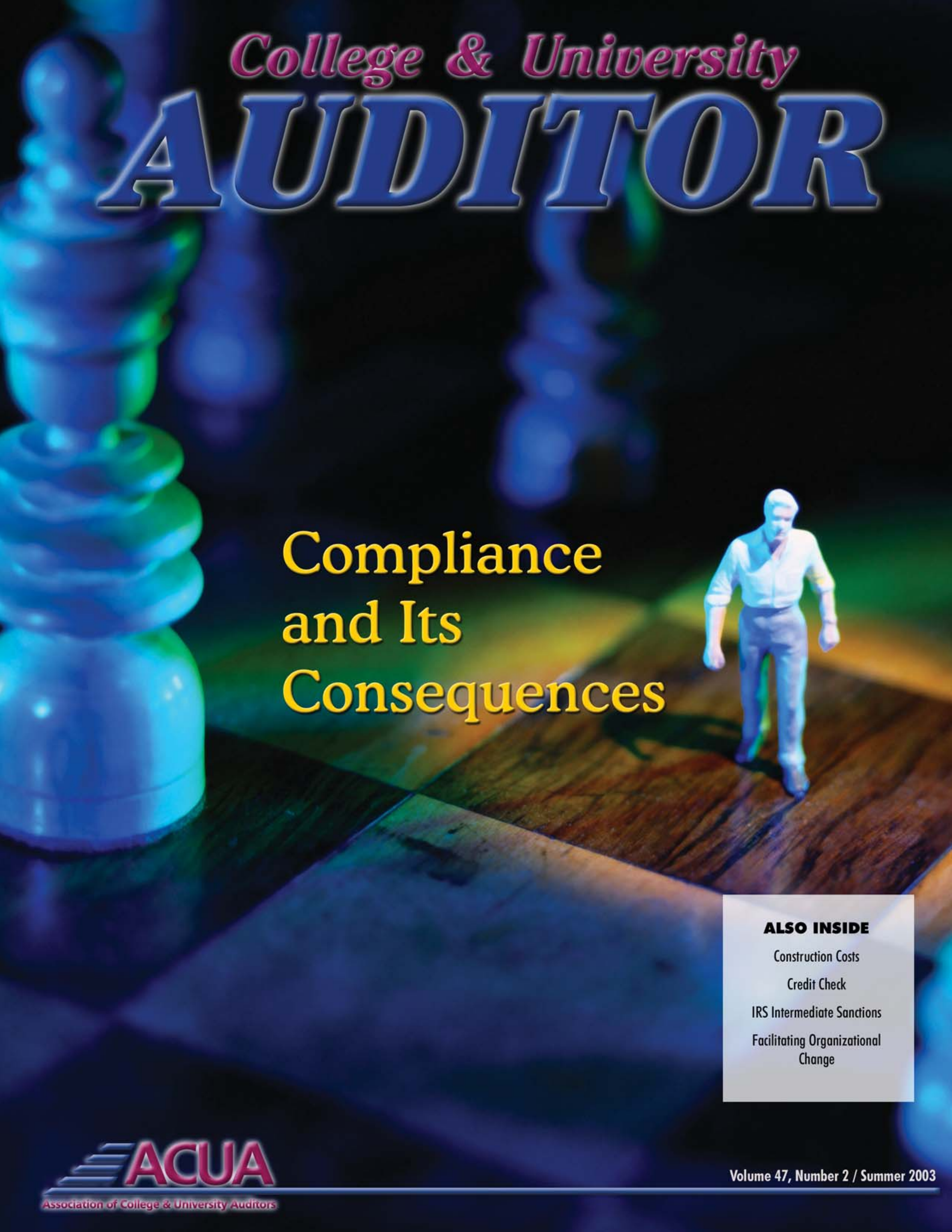


College & University AUDITOR

Compliance and Its Consequences

ALSO INSIDE

Construction Costs

Credit Check

IRS Intermediate Sanctions

Facilitating Organizational Change

ACUA

Association of College & University Auditors

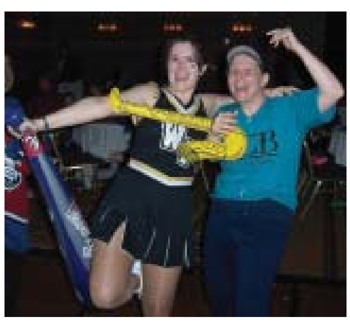
Volume 47, Number 2 / Summer 2003

2003 Midyear SCORES BIG!

The Board meets on Saturday and Sunday. Above are the board and committee chairs at work on Saturday. It was a full agenda with a lot being accomplished.

The two and a half day workshops attract 20-45 students per class. The workshop format meets our members' needs for in depth training on audit-related topics, many of which center around audit as it applies to our unique, higher education environment.

The traditional Sunday evening reception welcomes attendees with a great networking event. Above: Four attendees share their auditing experiences. Below: Two proctors meet at the reception to compare notes on their workshops.



ACUA's own DJ, Rob Clark (far left), not only spins the tunes but demonstrates what getting involved is all about. This year's dinner dance theme was "sports" and this ACUA cheerleader (top middle right) brought other attendees into the act. James Hodge (bottom middle right), Midyear Director, joins the fun. Attendees (above) wave their balloons for the camera.

ACUA
Association of College & University Auditors

College & University Auditor is the official publication of the Association of College & University Auditors and is published three times a year in West Hartford, CT. ACUA members are invited to submit letters and original articles to the editor. Go to www.acua.org and click on the "how to" button for further guidelines. The copy deadline for the next issue is **October 10, 2003.** Please send your copy electronically to the editor in Word 95 (or higher) or text file format. The editor reserves the right to reject, abridge or modify any advertising, editorial or other material.

Send address changes to:
ACUA
342 North Main Street
West Hartford, CT 06117-2507

College & University AUDITOR

Vol. 47, No. 2 SUMMER 2003

Contents

Features

Departments

Choose to be the Best

By Betsy Bowers, Editor

What is the most powerful word? I suggest the word *choose.* Think about it. Every step of your day is a choice. You *choose* from which side of the bed you arise. You *choose* whether to get a glass of juice or to brew a cup of coffee. You *choose* what time to leave for work. You *choose* how you are going to react to situations at work. Auditees *choose* to be compliant to policies, rules and regulations, or to be noncompliant to these standards. Accordingly, your decisions really all hinge on how you *choose* to view each situation.

As internal auditors, we are constantly faced with compliance and the consequences for noncompliance. We have to *choose* how to address a situation; *choose* either a finding to management or, if the magnitude would warrant, intervention. Some of these *choices* may be very tough decisions. They are not usually assessments of right versus wrong, but rather right versus right. For example, is it right to "throw the book" at good employees who make dumb decisions that endanger a program, and is it right to have enough compassion to mitigate the punishment and give them another chance? Luckily, those levels of *choices* are usually reserved for management and not the internal auditor.

This issue of the *CandU Auditor* focuses on *choices* we make as internal auditors and issues that regularly confront us. Our authors have tried to educate the readers regarding compliance to contractual agreements, laws, regulations and good business practices. These writers provide insight concerning the *choices* you must make as your institution's internal auditor.

Once we issue reports with findings, our work is not finished. We must perform follow up to ascertain if the recommendations have been implemented. Don Holdegraver's article focuses on organizational change and its facilitation. This article provides tools that can help us work with our management to achieve desired outcomes.

For example, it is right to "throw the book" at good employees who make dumb decisions that endanger a program, and it is right to have enough compassion to mitigate the punishment and give them another chance.

As an internal auditor, I challenge you to be the very best you can be. This is probably the hardest *choice* you will ever have to make. No one else can do it for you. No one else can take that away from you. Only self-analysis can tell you whether you are the best you can be. To quote the late Rick Nelson, "You can't please everyone, so you gotta please yourself." You have to *choose* to be the best and put your best efforts forward.

Finally, over the next week, make the following four *choices*: *drink, steal, swear and lie.* DRINK from the cup of life and be thankful every day for your many blessings. STEAL a few minutes each day to help someone less fortunate than you. SWEAR every day to be a better person than you were yesterday. LIE down every night with a clear conscience and be thankful for your opportunity to live and work in higher education.

Increasing Auditors' Skills, Knowledge, and Competencies

By Rob Clark, President

As preparations are being finalized for what promises to be an outstanding ACUA conference in Nashville, September 14-18, a question each of us should be asking is, "Where *do* we get our 'training' as auditors?"

***Standard* 1210 – Proficiency**, states: "*Internal auditors should possess the knowledge, skills and other competencies needed to perform their individual responsibilities. The internal audit activity collectively should possess or obtain the knowledge, skills and other competencies needed to perform its responsibilities.*"

Having recently attended three other professional conferences, I am more convinced than ever that the specialized educational content, applicability of subject matter, extraordinary professional development, exceptional networking opportunities, and overall value we experience at ACUA conferences are unparalleled. What we have in ACUA is something very special and something worthy of our continued investment of energy and resources.

Having said that, I am equally mindful that ACUA cannot nor should it be the only source through which we as auditors "*obtain the knowledge, skills and other competencies needed to perform [our] responsibilities.*"

If we were to survey the membership to assemble a list of resources used to increase our individual knowledge bases, it would be voluminous. Given other professional organizations' conferences, seminars, publications and Web sites, there is no shortage of information on issues that impact our areas of responsibility as auditors. As ACUA strives to continue on its path of excellence in providing *the* best source of information for auditors in higher education, I believe we should be availing ourselves of a variety of sources to expand our knowledge.

One information resource that I believe may be underused by our members resides right there on our campuses—with the subject matter experts (SMEs) in various fields. Who better, for example, to help increase the auditor's knowledge, skills and competencies on areas of exposure, regulations and effective practice regarding human resource risks than the individual SMEs within the Office of Human Resources?

Consider the benefit of having the director of Information Security sit down with the internal audit staff and provide briefings on key issues, best practices and risk mitigation strategies for information systems. The auditor can take that information into account as he or she conducts audits of this subject area around campus.

When I have presented this idea to other auditors, it is sometimes met with resistance. The reasons I hear are:

1. **"It will show our lack of knowledge about the subject, thereby potentially decreasing our credibility."**

   Do we really think that SMEs around campus think that we are experts in every area of risk mitigation that our institutions face? Most information security professionals, for example, would be among the first to say that *they* have a hard enough time trying to keep up with all the latest threats — and they focus on that subject full time. If we present ourselves as know-it-alls, do we really think that the SME is not going to see right through that? How much better would it be for internal auditors to initiate the conversation with the premise that we *do not* know all we should and are seeking their collaborative assistance in providing the appropriate guidance as we conduct our reviews around campus?

2. **"I'm not a [fill in the blank] specialized auditor. I will stick to conducting the types of reviews in which I do have strong skill sets. That way, I know that I am helping to add value to my institution.**

Continued on page 4

Continued from page 3

After all, I *know* I am an expert in financial auditing."

That would be great *if* the only risks that your institutions faced fell into the category of financial risks. We know, however, the threat-scape of risks extends far beyond to include exposures within information systems, human resources, legal and regulatory areas, health and safety, public relations issues, etc. If we choose to provide audit coverage for our institutions only in areas in which we already have strong knowledge, skills and competencies, we will, by default, be leaving large areas of exposure unaddressed. I have a hard time seeing how that model helps ensure the audit staff is "performing its responsibilities" of assessing all aspects of institutional risk.

3. **"I don't know enough about the subject matter to know if the SME is telling me the truth. He might deliberately try to mislead me and misdirect me so that I don't end up looking at issues under his control."**

Yes, that is a risk; however, I don't think it is a large one. I am not advocating relying exclusively on the perspective of the SME, but rather, to use that as a starting point from which to expand our knowledge and skills. In the process, we gain more information that allows us to verify the accuracy of the SME information. Further, my experience has been that people enjoy sharing details of what they do and their area of expertise. When you approach the person as an expert, he or she will, most likely, relish that opportunity to demonstrate competency and knowledge.

When we ask for the SME's assistance in evaluating our risk assessment methodologies and devising pertinent audit steps, the SME then has buy-in to our overall audit approach. He or she then becomes a potential source of support and an advocate for internal audit. This approach also enhances receptivitiveness to audit recommendations, because we can share with our clients that our audit opinion is additionally supported by the operational office in which the SME resides.

For the sustainability of our profession, we need to demonstrate we are adding value to our organizations. One essential factor will be to continually raise the level of our "*knowledge, skills and other competencies.*"

If internal auditing is to position itself as management's eyes and ears, we should ensure that we are looking at and listening to the appropriate issues. Involving management and various SMEs in the process of focusing our audit approach provides an invaluable opportunity for collaboration. At the same time, it provides a fabulous opportunity for internal auditors to elevate their "*knowledge, skills and other competencies.*"

My vision would be for ACUA members, as they gain more insights into emerging issues and areas of operational risk, to begin to share some of these insights with the ACUA membership so that we can all benefit. ACUA's Web site has been going through some significant revisions and will be rolling out in the very near future. Members will see many new features including a section that would lend itself very well to this type of information dissemination. The responsibility for populating the Web site and contributing summaries of key issues is something that cannot be placed on one or even a few people. It is a responsibility we all must share. For the sustainability of our profession, we need to demonstrate we are adding value to our organizations. One essential factor will be to continually raise the level of our "*knowledge, skills and other competencies.*"

In a presentation I offered at a recent conference, attended mostly by chief information officers, I encouraged the CIOs to initiate conversations with and offer information briefings to their internal auditors. I encouraged them to consider ways in which they can work collaboratively so that their internal auditors could be in a position to offer more value-added audit coverage throughout their campuses. I would encourage my ACUA colleagues to be prepared for that call. I would add, however, that it would be much more effective if you were to make the call first and reach out in an effort to enhance your knowledge base.

There is still nothing that can replace the professional development opportunities at our ACUA conferences. Those attending the next annual conference will find this to be the finest yet and more focused than ever on equipping attendees with information that will help them add value to their institutions. In the meantime, however, let us not overlook the learning opportunities on our own campuses.

Maximize Your Investment!

Attend ACUA's

Annual Business Meeting

Wednesday
September 17, 2003
Nashville, TN

Don't miss this year's Business Meeting. This important meeting is when our newly elected board members take office. You will also hear about the progress ACUA has made in the past year and learn about the association's plans for the coming year.

There will be a door prize drawing and one lucky ACUA attendee will go home with a digital camera.

"Pickin' the Best"
in Professional Education Opportunities

By Lorna Bolduc, Executive Director

ACUA provides great educational opportunities at both the Midyear Seminar and the Annual Conference. This year's Nashville conference promises to be the best yet.

The Kick-Off

Our opening reception will kick off the conference on Sunday evening. This event gets better every year. In addition to the great networking, the exhibits are now open during the reception. Integration of the reception and the exhibits adds a new dimension to the reception – education, and to the exhibits – entertainment.

Exhibits will be open Sunday evening through Tuesday noon. New this year will be short educational presentations by our exhibitors in the exhibit hall. Take advantage of this opportunity to learn more about the products and services being offered by our exhibitors and sponsors and don't miss the extra door prize drawings.

Education and Association Business Is Primary Focus

Monday's energizing general session will focus on leadership and team building. Back for the second time, Dr. Dale Henry of Your Best Unlimited will give us an entertaining look at successfully promoting change and improving our leadership skills. Check the conference brochure for Dr. Henry's description of the successful leader and then on Monday, September 15, listen to the stories driving home the points and striking a personal chord for auditors.

The tracks are packed with great CPE opportunities. You may find it hard to choose as there are seven to eight concurrent offerings. No matter which class you attend, you should walk away with new knowledge. The Annual Conference Program chair, David Coury, and his team of track coordinators continue to bring attendees a wonderful array of educational tracks at a price that doesn't bust already tight budgets.

Tuesday's keynote speaker is Dr. Michael Hoffman, executive director for the Center for Business Ethics at Bentley College. He will give us a lot to think about as he presents his views on the disastrous ethical scandals that have undermined public trust. Tuesday's session will also include the presentation of ACUA's coveted membership awards and scholarships.

Wednesday is a busy morning at every ACUA annual conference. We start the day with our annual business meeting. This important event is always a milestone for ACUA as it is when our newly elected board members take office. Members hear first-hand about the progress ACUA has made in the past year and about the prospects for the coming year. Be there! Maximize your institution's investment in ACUA by increasing your awareness of what the organization is doing.

Wednesday's keynote speaker is ACUA's very own Dr. Rick Whitfield. He will address the changing business environment and offer answers to difficult questions. Can models from the for-profit sector be adopted into the core leadership and management processes at colleges and universities? Who will champion the discussion, evolve the model and develop a common language for holistic consideration of institutional-wide risks in higher education institutions? You'll want to join us on Wednesday for Dr. Whitfield's perspective.

Networking After Hours

Our networking calendar is also full. In addition to Sunday's opening reception, we have planned several optional tours, transportation to shopping and dining, and our traditional dinner dance. Everything is outlined in the conference brochure (available online at www.acua.org). Take advantage of the great location to explore many of the notable Nashville sites. The best part is other ACUA attendees will be taking advantage of the same sightseeing opportunities so you'll be in great company.

Pickin' ACUA

The conference will be here before you know it and over quicker than you'd like. Don't miss the 22 CPE credits, networking with your colleagues from around the world, and socializing with the ACUA family. If you're new to the ACUA family, don't worry. We'll be working hard to make sure you feel right at home.

If you haven't registered, do it now at www.acua.org. Join us in Nashville, TN, where we'll be "Pickin' the Right Path…Working in Harmony."

Nashville
PICKIN' THE RIGHT PATH
WORKING IN HARMONY
September 14-18, 2003

Analysis of Construction Costs

By Paul D. Donovan, Tofias PC

Introduction

Many colleges and universities have embarked on multimillion-dollar capital improvement and building programs in recent years. This is a specialized area and some financial managers responsible for overseeing these projects may not possess the detailed knowledge of construction accounting, nor have the resources available to properly oversee all financial aspects of the projects. Further, inserting certain additional language into the standard construction contract agreement (construction agreement), whether in the form of a stipulated sum or cost reimbursable type contract, such as those provided by the American Institute of Architects, may result in cost savings to the owner. These provisions generally set forth certain additional criteria as to the specific cost of the work, as defined below, that are reimbursable and what costs will be excluded altogether. These provisions also provide a benchmark for the college's internal auditors and others in determining whether the costs billed to the project are reimbursable to the contractor or the construction manager (CM).

Construction agreements that contain language that is ambiguous or is silent concerning key issues can often lead to disputes between the contractor and the owner. This may result in further difficulties, particularly in instances when the contractor/CM who has already been paid by the owner must then try to recover overcharges, damaging what has otherwise been a good working relationship between the parties. Therefore, consideration must be given to addressing these issues during the contract negotiation stage to ensure that the contractor/CM (a) is cognizant of what costs are allowable and (b) identifies other expectations, including the owner's right to audit the costs, as well as the requirements of the contractor related to the agreement.

Construction agreements that contain language that is ambiguous or is silent concerning key issues, can often lead to disputes between the contractor and the owner.

This article will discuss different types of construction agreements. Based upon my accounting experience, I will identify costs that commonly are overcharged to projects and suggest language that an owner should include in a construction agreement.

Types of Construction Agreements

Fixed Price (Stipulated Sum) Contract – With this form of agreement, the contractor/CM guarantees to perform the work for a stipulated lump sum amount, subject to additions and deductions by change orders, and bears the risk if the costs incurred to perform the work exceed the stipulated contract amount. If the actual costs are less than the stipulated contract amount, then the contractor will realize greater profits. Generally this form of construction agreement does not provide the owner with a right to audit, except for costs related to changes in the work (change orders) discussed below.

Cost Reimbursable – Guaranteed Maximum Price Contract – The contractor/CM agrees to perform the work for a guaranteed maximum price (GMP), subject to additions and deductions by change order, based upon the allowable costs plus a fee, which is either a fixed amount or a percentage of the cost of the work. If the costs exceed the GMP, then the contractor bears the excess costs. If the costs are less than the GMP, the savings revert back to the owner or are shared in an agreed-upon proportion, as defined in the construction agreement between the owner and the contrac-

Continued on page 8

Continued from page 7

tor. By having a cost savings provision in the construction agreement, there may be an additional incentive to the contractor/CM to ensure that the project comes in under budget. This form of construction agreement also helps ensure that the owner is only paying for the cost of the work, with some negotiated fee as provided by the agreement. In agreements without a GMP, the contractor/CM is reimbursed for all allowable costs incurred plus a fee.

Cost of the work is generally defined in the GMP construction agreement as actual costs rather than an estimate or a reserve. While the contractor's method of allocating or charging costs to a project may be in compliance with generally accepted accounting principals (GAAP) for financial reporting purposes, it may not necessarily be in compliance with the contract provisions that mandate actual costs. When the construction agreement contains specific definitions within the contract provisions regarding what costs are to be included and excluded, scrutiny by an auditor often results in substantial adjustments to the costs submitted for reimbursement by the contractor, with the owner paying only for the actual cost of the work.

Unit Price Contract – This form of construction agreement is used when the contractor performs the work at a fixed price per unit of output. The primary issue to focus on with this type of contract is to ensure that the number of units or quantities performed has been correctly calculated. Generally, this form of construction agreement is used for projects such as highways or when large quantities of work will be performed and the exact quantities to be completed are not known until the work is finished.

Potential for Cost Recovery

Areas where there is a high potential for cost recovery by the owner, particularly using a cost reimbursement contract agreement (GMP) are identified below.

Components of Labor Rates

The components of labor rates generally include the employees' base salaries together with the labor burden. The labor burden (or overhead) includes benefits customarily associated with the base salary, such as vacation and holidays, sick and personal leave, social security and unemployment taxes and retirement benefits. A key concept to consider in determining whether a cost should be included in the labor burden is whether the benefit is mandatory or discretionary. Examples of discretionary costs include a cash bonus paid to an employee or a contribution to a profit-sharing plan.

The cost of labor charged to a project directly by the contractor/CM may be a significant portion of the project costs when the contractor/CM self-performs a substantial portion of the work, rather than retaining subcontractors to perform this work. (Contractors who do not self-perform work or perform little work are generally referred to as construction managers.) The contractor/CM may charge labor to various categories of work such as the general conditions, the managerial and administrative costs of the project to specific job tasks, line items or to change orders.

One approach in determining the contractor's labor rates (base salary and labor burden) or a labor burden multiplier is to use the bottom-up method. This method requires an analysis of the labor rates of all or a sample of the contractor's employees assigned to the project. This method will determine the allowable hourly labor rates for each employee, which will then be used by the contractor/CM to charge the project. This method can also be used to develop a labor burden multiplier by calculating the average labor burden divided by the average base salary. This factor is then multiplied by the employees' base salaries to calculate the hourly labor rates. When the contractor employs union employees, this will facilitate an analysis of the costs, as many of their benefits are

Continued on page 9

Continued from page 8

established by the union contract and wage agreement and are generally not subject to analysis or adjustment.

An employee's base salary is easy to confirm; therefore, most cost of the work audit issues revolve around what is included in the labor burden. Problem areas with the components of the labor burden include the following.

Payroll Taxes

Federal and state laws impose caps on the amount of payroll taxes that an employer must pay on behalf of its employees. Many contractors and their subcontractors ignore these statutory limits and compute an hourly rate as if there were no limits. This can greatly inflate the labor rate and result in substantial overcharges to the project. For example, the Commonwealth of Massachusetts unemployment tax assessment is capped at $10,800. The amount of the tax rate is based upon past claims made by workers against the company subject to both a minimum and maximum rate. Assuming a tax rate of 6%, the maximum amount of tax to be assessed by Massachusetts would be $648 per annum ($10,800 x 6%). In many instances, the contractor/CM and subcontractors err and apply the 6% to the employee's total salary in the labor burden, ignoring the statutory limitation. Similarly, social security taxes are assessed in 2003 on the first $87,000 of wages, and federal unemployment taxes are assessed on the first $7,000 of wages. Incorporating statutory caps in the construction agreement may limit the amount of labor burden overcharges to the project and will certainly facilitate post audit recovery.

Workers' Compensation Insurance

Usually the contractor/CM will purchase a policy from an insurance carrier that sets forth the rates for each classification of employee (i.e., laborer, carpenter, clerical, project manager, etc). To verify the actual cost, it is necessary to obtain a current copy of the premiums for the policy after the insurance carrier has audited the contractor's workers' compensation claims and adjusted the rates based upon the contractor's experience factor. Under this method it is fairly easy to determine the workers' compensation insurance rate for each employee and the amount to be included in the labor burden.

The contractor/CM that is self-insured and/or will obtain workers' compensation insurance excess coverage policy with high deductibles per occurrence and per aggregate (such as $250,000) will usually establish a reserve. This liability includes the contractor's estimate of current and future liability at that time. The contractor/CM will use it to calculate the amount of workers' compensation insurance to be included in the labor burden. However, the reserve amount is not necessarily the actual cost of the workers' compensation insurance.

The actual cost of the workers' compensation insurance should be calculated by first analyzing the cost of administering the insurance program and the amount of the claims paid to injured employees for the prior few years to determine a trend and a cost using a weighted-average method. The costs of administering the program may include all or a portion of the contractor's insurance administrator's salaries and benefits, fees paid to third parties to administer the program and/or the cost of the excess coverage policy. Calculating an appropriate workers' compensation insurance cost to include in the labor rate burden is problematic, as it requires a detailed knowledge of the contractor's insurance program and reasonable and valid assumptions based upon this knowledge. This calculation, however, may result in a substantial reduction of the workers' compensation insurance cost to be included in the labor burden and, correspondingly, the labor rates.

A recent trend in the construction industry is for the owner to include the contractor's employees and the subcontractors' employees in an Owner's Controlled Insurance Program (OCIP). Pursuant to the provisions of the OCIP, the owner pays the costs of the workers' compensation insurance for these employees and is reimbursed by the contractor and subcontractor for the amount that they would have paid for the insurance coverage. Assuming that the owner obtains lower rates from

Continued on page 10

Continued from page 9

his insurance carrier, then the owner will incur lower costs in comparison to those the contactor and subcontractor would have charged to the project. There have been instances where I have determined that the workers' compensation insurance costs were included in contractor's labor rates used to charge the project, although the contractor's employees were covered under the OCIP. This resulted in significant overcharges to the project and a corresponding adjustment.

Employer Pension and Profit Sharing Contributions
Often the contractor will include in the labor burden the amount of maximum contribution percentage required by the applicable retirement plan. Analyzing each employee's contribution may determine that either he or she is not enrolled in the plan or has elected a lesser amount of contribution than the maximum allowed by the plan provisions. In this situation, the employer's matching contribution will be either zero or a lesser amount than the maximum percentage.

Overhead Disguised as Labor Burden
A detailed analysis of the labor rates will also reveal whether other non-reimbursable costs have been included, such as (a) general liability insurance, (b) automobile insurance for employees without a company vehicle, (c) umbrella insurance, (d) computer costs, including the total cost of operating the contractor's computer department, (e) maintenance and repair expenses, (f) training and safety costs, (g) accounting costs, (h) materials, (i) travel and lodging, (j) parking costs and (k) truck expense. The provisions of the construction agreement should address what costs are to be included in the labor rates and what costs are specifically excluded. Some of these costs, such as general liability and umbrella insurance, may be appropriate project costs. However the better practice is for the contract provisions to require that these costs be listed as separate line items in the project budget based upon projected revenues from the project (i.e., $2.56 per $1,000 of revenue) rather than concealed in the labor burden.

Terms and Language in Construction Agreements

Change Orders
A change order is an amendment to the construction agreement, agreed to by the owner, contractor/CM and architect, which usually relates to increases or decreases in the scope of the work, adjustment of the contract sum and/or the time by which the work must be performed. Accordingly, the threshold issue is whether the work to be included in a change order has already been included in the base contract and, therefore, no change order is warranted. Certain costs of the contractor such as supervision, management, drawings, tools and supplies are generally not included in the change order but are reimbursed through the mark-up for overhead and profit discussed below.

Hourly labor rates for both the contractor and the subcontractors are a major issue in analyzing change order costs, regardless of the form of construction agreement, and an analysis of the rates generally results in finding substantial overcharges to the project. The components of the hourly labor rates should be analyzed for the contractor's employees (as discussed previously) and hourly labor rates calculated and compared to the amounts charged to the project. Generally, it is beneficial to analyze the labor rates of the contractor's subcontractors. This may be accomplished by requiring that the contractor/CM obtain from each of its subcontractors a summary of their labor wages and the labor burden for each employee or class of employee to be charged to the project.

There have been instances where I have determined that the workers' compensation insurance costs were included in contractor's labor rates used to charge the project, although the contractor's employees were covered under the OCIP. This resulted in significant overcharges to the project and a corresponding adjustment.

Consideration should be given to inserting language in the construction agreement requiring specific supporting documentation for each type of change order.

- A lump sum change order is a change order performed at an agreed-upon amount. The support should include a detailed take-off of the costs by item, listing the quantity and respective unit cost of the material, labor and equipment. It should also identify the amount of the mark-up as a separate amount.
- When a change order is for time and materials, the cost is reimbursed for the actual cost of the work including labor, materials, equipment and subcontractor costs. The support should include time cards/sheets/work orders signed by the owner's representative and copies of the invoices for material, equipment and supplies. For that portion of work being performed by a subcontractor, a similar detailed breakdown of each subcontractor's costs should be provided for analysis.

Fees (Mark-Ups, Profit and Overhead)
The GMP construction agreement should establish the amount of the contractor's fees for the project. The contractor's fee may be expressed as a lump sum or percentage of the cost of the work. For change order work, the contractor or subcontractor performing the work typically receives a mark-up rang-

Continued on page 11

Continued from page 10

ing from 10% to 15%. In addition, the contractor or subcontractor not performing the work also receives a mark-up that ranges from 5% to 10% on the work performed by the subcontractor or sub-subcontractor subject to a maximum amount or percentage. It is also advisable to define the allowable fee for change order work in a Fixed Price (Stipulated Sum) contract and Unit Price contract. This will mitigate the possibility of excessive fees being paid to the contractor/CM and subcontractors. In some GMP contracts, in lieu of a mark-up, the contractor will receive a fee expressed as a percentage of the work which may or may not be the percentage of fee on the base contract work. The mark-up allowed to a contractor and subcontractor is generally intended to provide reimbursement of the overhead and a reasonable profit on the work included in the change order. The calculation of the fee and mark-up must be analyzed to determine compliance with the contract agreement.

Allowances and Contingencies

An allowance is generally included in the construction agreement for work that may or may not have to be performed or when the quantity of work to be performed cannot be specifically identified. For example, the owner may not yet have decided between a wood floor and a vinyl floor for the building. The potential cost of the work is addressed in the construction agreement budget by providing an allowance for that work. Another example would be when traffic control (police detail) may be required at the project site, but the time required is not known.

A contingency is included in the construction agreement generally to address conflicts regarding scope of work items, to provide the contractor/CM with the financial resources to maintain the work schedule and to deal with other unknowns, particularly in situations where the plans and specifications are not one hundred percent complete at the time of the signing of the construction agreement. An example is the removal of contaminated soil from a site. Initial tests may provide an estimate of the quantity to be removed but the actual amount cannot be determined until the excavation and removal are complete. The owner will allow the original estimate in the construction agreement and a contingency for the potential additional work. The contingency is generally available to the contractor to use in the prosecution (execution) of the work.

The key issue here is to make certain that the allowances and contingencies are only being used as intended by the owner and should not used by the contractor to conceal overruns on other project work. The contractor should be required by the construction agreement to maintain detailed records to support its use of the allowances and contingencies. Incorporation of provisions in the construction agreement that specify when and whose approvals are to be obtained from the owner to allow the contractor to charge costs to the project for allowances and contingencies will aid in reducing unauthorized costs charged to the project. The construction agreement should also specify whether the unused allowances and contingencies revert directly to the owner or are shared with the contractor.

Acknowledgement: Special thanks to Victoria Escalera, Brown University Internal Auditing director, and Marshall Goldberg, director at Tofias and Practice Leader of the Construction Services Group for their constructive comments.

About the Author

Paul Donovan is manager with Tofias PC of Cambridge, Massachusetts. You may reach him at pdonovan@tofias.com.

Credit Check

By Phillip Hurd, Georgia Institute of Technology

In the early-morning hours in a dark office, the only thing stirring is the hard drive on the credit card transaction server. The air in the room is still. Outside, a security guard checks the door; all is secure. Within the office, the only light on is a light on the front of the server—one little light. It is 3:22 a.m.; the light begins to blink wildly—blink, blink, blink . . . For 10 minutes, this continues. It is 3:32 a.m., and the light stops blinking. Outside, a security guard checks the door; all is secure. What just occurred was a white-collar crime. A hacker just stole 200,000 credit card numbers. Within a few days, more than 10,000 people will experience credit card fraud, thousands of retailers will ship merchandise to fraudulent customers, and the credit card associations will lose millions of dollars. It does not stop there. Thousands will have their identity stolen, and that same hacker will scan many more machines looking for credit card numbers. This is a scenario becoming all too common for higher education, business and government.

While the above is a dramatization, Georgia Tech recently experienced the real thing. Last March, a hacker broke in and stole some 60,000 records that included credit card numbers and other personal information. While many details are beyond the scope of this article, procedures followed and lessons learned by Georgia Tech should help those who may face a similar situation. As higher education internal auditors, we have a special responsibility to ensure that we assess how well our institutions are positioned to handle such 21st-century electronic risks. Credit card theft, electronic commerce crime and computer crime are growing threats to academic institutions. Internal auditors must design audits to assess controls for preventing such crimes. The procedures and lessons learned at Georgia Tech can be integrated easily into traditional operational audits. With that in mind, this article closes with a list of audit points that may enable your institution to operate from a position of strength in these key control areas.

The Issues

Primarily due to institutional culture and academic freedom, most colleges and universities have a "distributed computing architecture." That means most computing power is located not in a central computing facility but in the hands of departments, schools, colleges or other local units. With distributed architecture, information security becomes exponentially harder to manage. Quite often, levels of security vary greatly among units. This is why having a good information security policy is extremely important. In addition, higher education institutions are known for having large bandwidth connections to the Internet, making it more difficult to track individual users or machines. Hackers thus find a more lucrative target. A large bandwidth also makes it more difficult to use an intrusion detection system to find a suspect file transfer or other anomaly.

The World Wide Web began changing the way business, government and higher education conducted operations in the early 1990s. We are now faced with unprecedented complexity in our administrative systems, and institutions of higher education have a tough time responding. Moreover, in higher education, information security is often viewed as detracting from academic freedom. Because higher education dedicates so much of its resources to the academic environment and minimizes attention to the administrative environment, controls to support 24/7 electronic monitoring are not a top priority. As a result, higher education institutions are prime targets for hackers, crackers and all types of white-collar criminals. Because internal auditors are often considered the vanguard of defense against traditional crimes such as fraud, we must apply those same skills to the distributed computing environments of higher education. A first step is to enable management to understand and assess the high risk faced by colleges and universities.

The Risks

Anything that can disrupt an organization's ability to achieve its strategic and business objectives is a risk. Theft of person-

Continued on page 13

Continued from page 12

ally identifiable information is a huge risk to higher education because of the damage to reputation, financial impact and other liabilities. The need to protect sensitive information arises not only because of white-collar criminals but also because of the requirements of the Family Educational Rights and Privacy Act (FERPA), the Health Insurance Portability and Accountability Act (HIPAA), the Gramm–Leach–Bliley (GLB) Act, the USA Patriot Act (USAPA) and state laws. Put simply, institutions of higher education face a myriad of risks because of all the personally identifiable information on our networks. Additionally, significant increases in white-collar crimes such as credit card theft have led to other implied obligations. For example, in 2001 VISA USA put into effect its Cardholder Information Security Program (CISP), which states that all merchants who store credit card information must comply with Digital Dozen. In April 2003, MasterCard released a new information security program and service for information security assurance. Most other major credit card associations will likely follow suit as the costs of credit card fraud rise.

The risk impact comes not only from information exposure but also from the large amount of personnel hours and information technology resources required to correct the situation(s) that led to a compromise. After all, we must continue to accept credit cards after a compromise occurs. Georgia Tech has an incident response plan in place for addressing such compromises at the executive level. The plan was quickly put into action. While the immediate technical hurdles were addressed, the lingering effects of this compromise, the follow-up external audit and the bad press from the initial compromise are still ongoing. This incident will easily top $100,000 in monetary damage, and we are still counting.

Dealings with the Associations

Georgia Tech's first action after a critical compromise has been identified is to assemble a group of the key stakeholders and assess the situation (see diagram, which is also provided at http://www.audit.gatech.edu/IAcollabrative2.wmf). The group then decides the next steps. In the case of our recent compromise, this group decided to contact law enforcement and the credit card associations. While no direct evidence showed the cards had been used fraudulently, Georgia Tech suspected a hacker had gained access to the database housing the card information. That opened up the Pandora's box of requirements that had recently gone into effect—otherwise known as VISA's Digital Dozen, which are 12 rules for handling stored credit card information.

The Digital Dozen

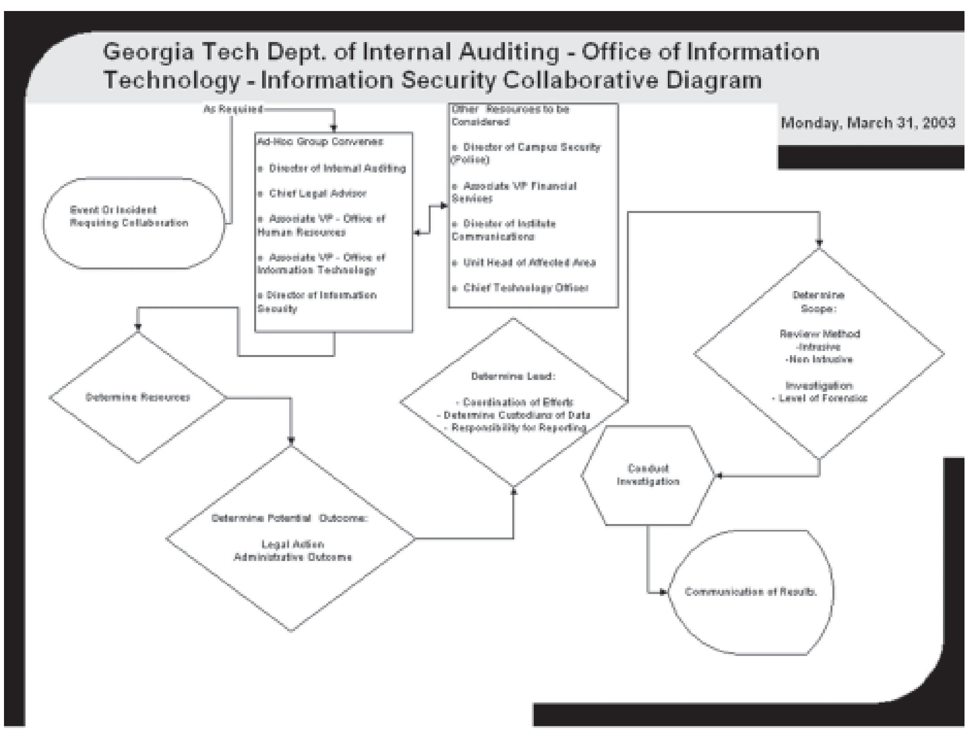
1. Install and maintain a working firewall to protect data.
2. Keep security patches up to date.
3. Protect stored data.
4. Encrypt data sent across public networks.
5. Use and regularly update anti-virus software.
6. Restrict access by "need to know."
7. Assign unique ID to each person with computer access.
8. Do not use vendor-supplied defaults for passwords and security parameters.
9. Track all access to data by unique ID.
10. Regularly test security systems and processes.
11. Implement and maintain an information security policy.
12. Restrict physical access to data.

For more information, go to http://www.usa.visa.com/business/merchants/cisp_index.html?it=h2_/index.html.

When the card associations were first contacted, they had several questions and, of course, expected the card numbers. The requested information and questions were:

- Merchant number.
- What is the physical location of the compromised server?
- If a Web server, what are the associated URL(s)?

Continued on page 14



Continued from page 13

- What date/time, based on available information, did the unauthorized intrusions begin?
- How many intrusions have been detected?
- How were the intrusions detected?
- What data were in the compromised files (name, address, account number, etc.)?
- Was the 3-digit signature panel code (a.k.a. CVV2, CVC2, CID) stored in the compromised file?
- How many account numbers were compromised?
- Was the data stored on a Web server? If yes, what type of server?
- What type of database was the data stored in?
- Was the data encrypted? What type of encryption?
- Based on the investigation to date, is it believed that the hackers were able to export the data out of your system?
- Has your organization been contacted by anyone claiming responsibility for the intrusion? Please provide details.
- Has law enforcement been advised?
- Has or will a statement be made to the media regarding this incident?
- Do you plan on contacting the affected customers directly?
- Provide a narrative describing in detail the steps that your organization is taking to investigate this incident.
- Provide a narrative describing in detail the steps that your organization is taking to correct and mitigate further exposure to unauthorized intrusions.

All card associations asked questions a little differently, but all wanted the same information. VISA immediately wanted a forensics audit to determine not only the cause of the compromise but also where the initial intrusion originated. VISA also had a secure Web site for uploading card information and required a follow-up external audit with an action plan showing the date for expected completion of each action item. That audit was to focus not only on the actual place that the compromise occurred, but also on the entire campus network and areas that stored or processed credit card information. (MasterCard presents its best practices at http://sdp.mastercardintl.com)

Dealing with Law Enforcement

Before card associations are contacted, it is important to understand when law enforcement should be called. First is best. The Federal Bureau of Investigation (FBI), state agencies and the Secret Service have an interest in this type of white-collar crime. The FBI is a good place to start, and they can contact other agencies as needed. The FBI regional computer crimes squad can be reached through the local FBI office (see www.fbi.gov).

Many states now require specific due diligence steps in protecting credit card and other sensitive information (see http://www.stopidentitytheft.org or www.findlaw.com). Once law enforcement has been contacted, they will provide the next steps for how they want to conduct the investigation.

Dealing with Clients

Georgia Tech's clients were patrons of the Robert Ferst Center for the Arts, and we decided to contact each patron and inform them that their personal information and credit card numbers may have been compromised. To do this, we sent letters to nearly 60,000 people and set up a small call center, e-mail address, and a Web site: http://www.patronservices.ferstcenter.org. The Web site was extremely helpful in providing instructions on how to protect against loss.

Audit Points

The best way to protect your institution is by not having to respond to an intrusion. This may seem like a monumental task at times, but here are some audit points that may help:

1. Identify all places on campus where credit card payments are accepted or processed.
2. Identify all places that store credit card information.
3. Perform audits for compliance with VISA CISP/MasterCard best practices.
4. Confirm that all critical credit card information is managed by a competent, trained systems administrator.
5. Ensure shared networks have proper access and authentication controls to protect the segment of the network in which credit card information is stored.
6. Confirm that there are proper controls and an appropriate destruction process for paper documents containing credit card information.
7. Verify there are vulnerability scans to immediately trap and identify intrusions or attacks.
8. Make sure that there is a business need for all stored credit card information.
9. Have a monitoring plan (intrusion detection, scans, etc.) to queue incident response teams.

The increasing complexity of the information technology environment combined with ever-increasing demands of students, employees and the general public make it difficult to set priorities and make choices. In the final analysis, it does not matter whether "Brand A" or "Brand B" was chosen for a firewall or which operating system was used on the server. What really matters is that your institution is protected, as much as possible, against the theft of credit card and other sensitive information.

About the Author

Phillip Hurd, CISSP, CISA, CBM is associate director IS auditing at Georgia Institute of Technology. You may reach him at phil.hurd@business.gatech.edu.

IRS

Intermediate Sanctions—and How to Mitigate the Risks

By Mary Lee Brown, Chairperson Governmental Relations Committee

What are IRS intermediate sanctions? They are excise taxes imposed by the IRS on *certain individuals* as penalties for use of substantial influence over certain tax-exempt organizations for inappropriate personal gain. Can they hurt me? Yes, perhaps.

What Are They?

Intermediate Sanctions were created in the Taxpayer's Bill of Rights 2 (TBOR-2) federal tax act. Section 4958 was added to the Internal Revenue Code by TBOR-2 in July 1996 with final regulations published on January 23, 2002. Prior to TBOR-2 the IRS only had the option to revoke tax exemption of an organization as a consequence to individuals misappropriating charitable assets for personal gain. Understandably, the IRS was reluctant to use such an extreme penalty. Revocation hurt the organization, which was already a victim, rather than the responsible persons receiving inappropriate benefits. Intermediate Sanctions gives the IRS an effective "intermediate" solution to discourage certain individuals from misusing their influence over a tax-exempt entity for personal benefit.

Who Are These Individuals?

The regulations use the terms "*disqualified person*" and "*organization manager*" to describe the individuals subject to the excise taxes. A *disqualified person* is any person who was in a position to exercise substantial influence over the affairs of the tax-exempt organization at any time during the five-year period ending on the date of the transaction. This includes certain family members of the individual with substantial influence and also includes corporations, partnerships or trusts in which a disqualified person owns more than a 35% interest. Examples of disqualified persons: voting members of the governing body (e.g., trustees), CEOs, COOs, CFOs, treasurers and department heads that manage a discrete segment or activity of the organization that represents a substantial portion of the activities, assets, income or expenses of the organization. An *organization manager* is any officer, director, trustee or any individual having powers or responsibilities similar to those of an officer, director or trustee regardless of title (e.g., approval authority). Generally the organization manager is any individual with the authority or apparent authority that knowingly participated in the transaction on behalf of the tax-exempt organization.

The sanctions are imposed when there has been a determination of an "excess benefit" transaction. An excess benefit transaction is any transaction in which an economic benefit is provided and approved, directly or indirectly, to or for the use of any "disqualified person" where the value of the economic benefit exceeds the value of the consideration received for providing the benefit. In a nutshell, the IRS intends to use Intermediate Sanctions as a deterrent to certain inappropriate transactions in tax-exempt organizations.

Can They Hurt Me?

If colleges and universities are not adequately prepared, their disqualified persons and organization managers could be subject to substantial personal, monetary penalties, and the organization could be harmed by the required public disclosures and unwanted adverse press. Examples that have been raised on IRS examinations include:

- Reasonableness of compensation arrangements including fringe benefits (reported and unreported),
- Reimbursement of personal expenses,
- Contractual arrangements and vendor relationships,
- Advances characterized as loans,
- Payment of personal expenses of family members,
- Rental agreements,
- Property transactions (real and personal, sales, purchases, and uncompensated use),

Continued on page 16

Continued from page 15

- Personal use of property owned by tax-exempt organization (e.g., cars, labs),
- Medical directorships, and
- Joint ventures.

Higher education institutions can take steps to create a safe harbor for compensation arrangements and transfers of property transactions under the "rebuttable presumption of reasonableness" safe harbor. Essentially, this provides that payments under a compensation arrangement are presumed to be reasonable, and a transfer of property, or the right to use property, is presumed to be at fair market value if the following conditions are met:

1. Advance approval by the governing body,
2. Reliance upon appropriate data as to comparability prior to the board making a determination, and
3. Adequately documenting the basis for the board's determination concurrent with making the decision.

Availing yourself of this safe harbor shifts the burden of proof to the IRS.

Excise Taxes and Corrective Actions

When there has been a determination of an excess benefit transaction, the disqualified person is assessed a 25% excise tax on the excess benefit. A 10% excise tax is imposed on organization managers who knowingly participate in the transaction (limited to $10,000 per transaction). There is an additional 200% excise tax to the disqualified person if the excess benefit is not returned to the organization within a prescribed timeframe.

The corrective actions required include repayment, by the disqualified person, to the organization of an amount equal to the excess benefit plus interest for the period the excess benefit was held and disclosure by the organization on IRS Form 990 annual information return of each excess benefit transaction and the amount of excise taxes paid. IRS Form 990 is readily available for public inspection directly via the World Wide Web.

One University's Approach

The University of Pennsylvania took a proactive approach and, in fiscal year 2003, launched an educational awareness initiative to inform its potential disqualified persons and organization managers of these new rules and sanctions. The initiative was the result of collaboration among representatives from the Corporate Tax Office, Office of General Counsel, Office of Audit and Compliance and the University Health System. The program educates individuals on the basic rules for Intermediate Sanctions, discusses who is at risk, explains how to identify the myriad events on campus that can cause exposure and outlines the steps necessary to provide protection under the "rebuttable presumption safe harbor." The sessions stress the importance of timely and proper documentation and highlight the detriments to tax-exempt universities involved in "excess benefit" transactions. The program includes a customized video with cautionary comments from The University of Pennsylvannia vice president of finance and treasurer and its vice president and general counsel. In addition the program uses a comprehensive slide presentation, various handouts that serve as ongoing reference and reminder resources, and instructions on whom to call on campus for help and questions. Higher education– specific case studies were developed for use in breakout groups during the educational sessions to help participants apply the Intermediate Sanctions rules. Finally, an Intermediate Sanctions Web page was created as a single location for tools, resources and information on the rules.

About the Author

Mary Lee Brown is executive director, University & Information Systems Audit at the University of Pennsylvania and serves as chair of the Governmental Relations Committee.

You may reach her at marylb@pobox.upenn.edu.

Facilitating Organizational Change—

REVIEW THROUGH PROJECT FOLLOW-UP

By Donald Holdegraver, University of Nebraska

The auditor has reached the end of the review project, the suggested management actions (to be taken) have been formulated, management's action plan has been presented and accepted, and the final report has been issued. *Now what?*

Is the internal auditor's job completed, or is the work just beginning? This is a defining question in an internal auditor's professional life. In many cases, the internal auditor will have to find the answer on her or his own because there is no stock answer.

Finding the Answer

To learn that answer, the internal auditor should first evaluate the role of the internal audit report. Ask the average internal auditor what the product of an internal audit is and the response in many or most cases will be "an audit report." A less common response will be that the product of an internal audit is "organizational change."

Let us challenge this assumption.

Premise – No matter how well written, how technically correct or beautifully presented, an audit report is in most cases just one of many pages to be handled by a typical operating manager on a typical day. The emphasis this report receives over others is wholly dependent on the importance the operating manager places on its content, and how it will assist the manager in getting through that typical day.

How does the internal auditor elevate the importance? An internal auditor, in completing the review project and developing the project report, can simplify the process of defining the answer to the initial question "Now what?" Building the entire review, reporting, and follow-up process around the concept of facilitating organizational change rather than "conducting an audit" helps elevate the importance.

The Report

The role the report plays must be that of a facilitation tool—part of a greater facilitation process and not an end product. A facilitation tool is one that moves individuals to action and is a catalyst for change. Reports cataloging sins will commonly get little consideration (i.e., dust gatherers). Reports that are efficiency and/or effectiveness idea generators focused on true operating risks will be accorded the status of action documents.

What makes an internal audit report a facilitation tool? This question is as difficult as our initial question. Every organization has its individual focus, hot buttons, corporate culture and approach to change. The internal auditor first must know, or try to know, the organization to determine what makes a report a facilitation tool in the internal auditor's organization.

Every organization has its individual focus, hot buttons, corporate culture and approach to change. The internal auditor first must know, or try to know, the organization to determine what makes a report a facilitation tool in the internal auditor's organization.

Certain points would appear to be universal. Few organizations or individuals are moved to true organizational change by accusation, finger-pointing, harsh or charged language, ultimatum or power play. Many articles and presentations have addressed the grammar and style aspects of audit report writing, so those concepts are not readdressed here. Explaining and obtaining buy-in about the risks and benefits, however, is a significant aspect of making a report a facilitation tool. If the report properly addresses the risks and benefits, organizational change will be the outcome—assuming the benefits are greater than the risks.

Consider the following reporting situation:

Continued on page 18

Continued from page 17

Finding— "File cabinets are left unlocked overnight."
Recommendation— "Lock the file cabinets every night."

As an operating manager, how would you receive and respond to this? *Is it likely to provoke real organizational change?* Maybe—for a little while.

A report that is a facilitation tool, however, will hopefully cause the operating manager to consider more than the physical fact that locks were not used. Rather, the operating manager's thoughts might gravitate toward:

- Are these files critical?
- Who has access after hours?
- What damage could be done by unauthorized access?
- Who might be harmed by release of these documents?
- Why is it in my best interest to secure documentation files?

The difference between the reaction in the first situation and the reaction in the second is the difference between the physical (use of lock and key) and the more abstract (the impact of information). When the report provokes the thought process in the second situation, the internal auditor is again on the way to solving "*Now what?*"

The Review

The concept of the report as a facilitation tool, however, does not actually emerge with the draft report document. It is but a step in a process that presumably has gone on throughout the review. It is communication and information exchange. It is discussing with operating management the impacts of issues as they are identified as well as development of workable solutions to those impacts. It is operating management seeing the importance and benefits of document security—not just being told to "lock the file cabinets."

The term *partnership*, though occasionally overused in recent years in internal auditing discussions, may be the appropriate descriptor for the concept of facilitation, through the review, the report and follow-up. Partnership implies working together for the common good, and what better good is there than organizational change that improves the efficiency, effectiveness and risk management focus of the organization? Partnership, facilitation, buy-in; all interrelated, and all focused on organizational change.

So, *where do we as internal auditors stand?* We have partnered with the operating manager. We have communicated and exchanged information during the review. We have confirmed the impacts with management of the issues we have noted. We have suggested management actions, and management has developed an acceptable action plan. And we have a well-written, technically correct, and beautifully presented project report.

At this point, the answer to *"have you done your job, or is your work just beginning?"* seems relatively clear. In the strictest sense, it is now up to management to follow through on the commitments made in the facilitation during the review and through the report. All the work that has been done has, hopefully, instilled in operating management the buy-in needed to assure management action and organizational change.

If done properly to this point, there may be no need for further work on the part of the internal auditor. Follow-up will only confirm the obvious; management has implemented organizational change based on the highlighted issues. We therefore return to our initial question, "*Now what?*", by looking at the follow-up process in more detail.

The Follow-up

The IIA Professional Practices Framework assigns a responsibility to internal auditors to follow up on management action toward implementing internal audit recommendations. Is there a blurring of independence and management responsibility here, however, which forces the internal auditor into a policing role despite the newer definition of internal auditing in the same Framework? It would appear there is a blurring; however, the key point is that the Framework does not define what the follow-up must be.

Using the overall facilitation approach, *what might follow-up be?* Let us first consider a 30-day status check concept useable on most if not all projects. Using our earlier file cabinet scenario, call the operating manager and ask, "How is it going with the document security implementation? Any unanticipated problems with taking the action you indicated in your action plan? Are you on target with your planned implementation date? Anything more I can do to help you get this change implemented? I'll check back with you in 30/60/90 days. Call me before then if anything unexpected pops up."

You have now fulfilled IIA follow-up requirements; you have reconfirmed your commitment to helping the operating manager achieve organizational change to which the manager agreed. You are continuing to facilitate that change. You can provide a status report to the audit committee if that is needed. And it took you less than 15 minutes!

> **Is there a blurring of independence and management responsibility here that forces the internal auditor into a policing role despite the newer definition of internal auditing in the same Framework?**

Internal audit purists might see this as a simplistic approach and that the only option is to do a follow-up audit of each recommendation. In a facilitative, non-adversarial environment, however, the need for a line-by-line assessment of recommendations are obviated through the facilitation process. Trust and action is fostered by facilitation because differences of opinion are resolved early in the process, not during the management action stage.

Continued on page 19

Continued from page 18

However, *what happens if after a specified period (e.g., 120 days) the agreed-upon management action has not been taken*? Much depends on the individual organization's approach to management action on internal auditor recommendations. In one organization in which I previously worked, audit follow-up reports could be issued every few months forever and nothing would happen to motivate organizational change. In another organization, the audit committee made it management's job to follow up and implement, and would "invite" to the audit committee meeting management team members who were unable to find time or justification to implement agreed-upon action plans—to explain why. In another organization, state law mandated certain response times.

The intent should be to establish follow-up practices that take the internal auditor out of the loop as the primary follow-up monitor. Internal audit seldom has authority to force change. Most internal auditors can do little more than point fingers and say "shame on you" for not implementing change. And, to a large extent, the internal auditor should not be able to do much more. The IIA Framework addresses that it's management's responsibility to manage, not internal audit's. Unfortunately, that does little to establish an environment for facilitating organizational change.

If the organization has an audit committee, the internal auditor may assist the audit committee in recognizing management's accountability, not internal audit's, for implementing organizational changes. It takes but a few calls from the audit committee to operating managers to encourage them to implement management action plans. When the audit committee (or senior administrators) holds operating managers accountable for corrective action, the internal auditor policing role is eliminated and replaced by a change support role. This situation also helps solidify a future partnership between operating management and the internal auditor to assure organizational change occurs as needed through management action.

If the organization is one that requires the internal auditor to be intimately involved in the follow-up process, there is still hope. If the internal auditor has facilitated well through the review and reporting process, few issues should arise to create follow-up controversy. The operating manager will have already bought into the need for organizational change (not the need for responding to audit reports), and will have taken proactive measures to implement management action plans resulting in organizational change. It is precisely in these situations that the facilitation approach is most important and most effective.

A Complicating Factor—Minimal Risk Issues

Of course, all the actions described to this point depend on one remaining factor—the nature of internal audit recommendations that have been made. With the demands on operating managers in higher education today, it is essential that recommendations made by internal audit positively impact the true risk environment of the organization, rather than being nuisance recommendations. All too often, internal auditors include in audit reports issues and recommendations that do not meet the risk test.

Each issue brought to management in the project report must be a true risk issue. Internal auditors have traditionally focused on compliance with rules, policies, procedures, guidelines, etc. This focus has led to inclusion of issues that have extremely limited overall risk.

Each issue brought to management in the project report must be a true risk issue. Internal auditors have traditionally focused on compliance with rules, policies, procedures, guidelines, etc. This focus has led to inclusion of issues that have extremely limited overall risk. Is the fact that two of ten purchase requisitions were not signed by the manager a true risk issue? Maybe, but more likely not. Is the imminent compromise of confidential or proprietary documents or information to competitors or outside media a true risk issue? Probably yes.

Knowing and addressing true risk issues is the stuff of value-added auditing, and the end result of facilitation during and after reviews. If facilitation is practiced consistently, the "*Now what*?" question becomes moot because risk-minimizing change becomes a practiced constant, and the need for follow-up is minimal to nonexistent. It allows operating management to focus on the real issues, while freeing the time of internal auditors to explore new and emerging risks, and begin facilitating change to address those risks.

The Premise Revisited—A Summary

The level of importance placed on the report page received by the operating manager, over the many other pages the manager receives on a particular day, is enhanced by using the facilitation process in reviewing, reporting and following up on operating issues. Facilitating organizational change throughout the review, reporting and follow-up processes will (1) enhance the probability of real organizational change occurring, and (2) make change become the norm and a positive part of continuing operations.

About the Author

Don Holdegraver, CPA, CFE is director Operations Analysis at the University of Nebraska–Lincoln. He has more than 24 years of internal audit experience, including 17 years in higher education. He may be contacted at dholdegraver2@uynl.edu.

ABACUS GAIN 2002 *Initial Results from ACUA's Third Triennial Benchmarking Survey*

By Steve Jung, Chairperson, Best Practices Committee

Background

Since 1995, ACUA's Best Practices Committee has carried out a voluntary benchmarking service for college and university auditors called ABACUS: Analytical Benchmarking for Auditors in the College and University Sector. Comprehensive surveys were carried out in 1995 and 1998, and results distributed to members in 1996 and 1999, with the results of a separate electronic "best practices" survey published in 2000.[1] In 2001, the ACUA Board decided to merge the third triennial ABACUS survey with the IIA's Global Auditing Information Network (GAIN) internal audit benchmarking program.

The ACUA Board decided to go this route in 2002 instead of carrying out our own ABACUS benchmarking survey because of the benefits associated with broader benchmarking with private industry internal audit functions, e.g., access to benchmarking data for not only other ACUA member schools but also for the entire universe of GAIN participants—over 750 organizations in 2001. GAIN offered other value-added services as well, such as Web-based surveying capability, fully electronic reporting, and regular access to the GAIN FLASH survey network, which carries out periodic issue-specific surveys with instant Web-based access to survey results.

In April 2002, ACUA member institution primary representatives received notice of the opportunity to participate in ABACUS GAIN 2002 at no cost (compared to the regular GAIN participation fee of $225 to $395 depending on reporting options selected). E-mail instructions were sent out regarding how to log on to the IIA GAIN Web site and complete the 2002 benchmarking questionnaire. During the three-month data collection window, 181 member institutions (43 private, 107 public, 13 international and 18 statewide systems) did so (approximately 45% of our 400 institutional members). In late August/early September 2002, GAIN e-mailed each of these institutions a comprehensive report in Portable Document Format (.pdf) allowing benchmarking comparisons to be made with the internal audit functions of the other ACUA participating schools, as well as internal audit functions in other industries, on almost 400 different dimensions broken down into the following categories:

A. General Institutional Statistics

B. Costs and Staffing

C. Audit Committee

D. Customer Satisfaction

E. Chief Auditing Executive (CAE)

F. Annual and Long Range Planning

G. Activities Audited

H. Audit Life Cycle and Resource

I. IT Auditing

J. Successful Auditing Practices

K. Continuous Improvement

L. Specialty Groups

M. Background Information

In this article, the first of three, the Benchmarking Committee is pleased to highlight some of the most interesting and potentially useful results from the 2002 survey. At the end of the article, we discuss the next two planned articles as well as opportunities for ACUA members to mine my additional results from the ABACUS GAIN 2002 database.

Survey Participation

Table 1 on the following page provides summary data on the ACUA member institutions that participated in the 2002 survey.

Continued on page 21

Continued from page 20

Table 1

Institution Type	#	Average Annual Revenues	Average Total Assets	Average Annual Expenses	Average FTE Employment	Average FTE Student Enrollment
Private	43	$802,673,746	$2,939,213,180	$787,539,712	6,867	11,517
Public	107	$604,507,831	$1,059,464,058	$572,950,094	5,516	20,778
Non-US	13	$245,561,007	$471,744,590	$251,378,927	3,192	30,863
Systems	18	$1,338,677,811	$7,786,833,804	$1,300,710,518	18,390	61,161
	181					

Table 2

Institution Type	Salaries	Travel	Training	Contracting	Other	Total Dept Costs
Private	$445,940	$2,519	$14,000	$60,486	$79,354	$578,421
Public	$297,355	$2,794	$7,763	$4,071	$34,378	$343,085
Non-US	$231,334	$3,867	$5,885	$34,733	$36,164	$288,405

In the analyses that follow, we have *omitted the data from the 18 statewide systems of higher education*, because their organization and functions are sufficiently dissimilar from those of the other institutional respondents to invalidate any comparisons that might be drawn. Note, however, that we are willing to make these data available, sans identifying information, for any ACUA member who wishes to do benchmarking within this specialized subset (or other subsets). See the last paragraph of this article for information on how to obtain the data.

Audit Department Statistics

Annual costs. Table 2 above provides information on the reported internal audit department annual costs for the 2002 survey respondents, averaged by type of institution.

Not unexpectedly, salaries represented the bulk of reported departmental costs (ranging from 77% at private and non-US institutions to 88% for public institutions). In contrast, only a small percentage (around 2%) of departmental expenses go toward training.

So that individual schools can better benchmark the size of their own audit function budgets, we calculated the average total internal audit departmental costs per $100M of institutional revenues and assets, and report those data in Table 3.

Note that the high average costs per $100M of revenue and assets for the non-US institutions shown in this table are heavily influenced by a few universities that reported very high internal audit department budgets relative to their revenues and assets, so the averages reported here may not be representative.

It might be useful to provide an illustration of how any ACUA member can use the above data in benchmarking. For example, Generic Private University's annual revenues in 2002 were $500,000,000. So GPU's Chief Audit Executive (CAE) could compare her 2002 annual operating budget ($300,000) against these norms by multiplying the average annual costs for private universities ($75,745 per $100 million in revenue) times 5, or $387,725. Her conclusion that her department's 2002 budget was below average by $87,725 would be justified.

Continued on page 22

Table 3

Institution Type	Average Annual Costs/$100M Revenue	Average Annual Costs/$100M Assets	Average Annual Costs/Prof FTE
Private	$75,745	$28,223	$97,542
Public	$84,346	$57,329	$69,255
Non-US	$161,518	$84,359	$61,324

Table 4

Institution Type	Average Prof FTE	Average Prof FTE/$100M Revenue	Average Prof FTE/$100M Assets
Private	6.01	0.89	0.33
Public	4.77	1.46	0.96
Non-US	5.23	3.11	1.58

Continued from page 21

Annual external audit fees. ABACUS GAIN 2002 also collected information on the amount paid for external audit fees, excluding any fees for co-sourcing or consulting services. On average, private institutions (38 reporting) paid $255,726, or .05% per $100M in revenues, and public institutions (76 reporting) paid $142,060, or .03% per $100M in revenues. For non-US schools, the corresponding figures were $92,867 (13 reporting) and .06%, although the mix of audit services represented may be different than that for the US schools.

Department size. Table 4 (previous page) shows the average size of participating departments by institution type in terms of full-time equivalent (FTE) professional auditors (including the CAE). The table also illustrates the average size of department professional staffs per $100M of institutional revenue and assets.

These data can be especially useful for benchmarking the size of an internal audit department. For example, for GPU mentioned above, its $500,000,000 annual operating revenues could be used to determine that, all other things being equal, the average internal audit staff would number approximately 5 times .89, or 4.9 FTE.

The ABACUS GAIN 2002 data on department size by institution type are also displayed in Chart 1 above.

Collectively, based on these responses by 163 member institutions, it is clear that in 2002 the bulk of ACUA's member internal audit departments were small to medium (overall, 48% have three or fewer professional staff and 67% have five or fewer).

Combining the data on total average annual departmental costs and size produces another set of interesting benchmarking statistics, shown in Table 5.

Staff salaries. The IIA GAIN questionnaire asked respondents to report on high, average, and low annual salaries for audit directors, supervisors, staff auditors, and clerical/support staff.

Table 6 presents a summary of the ACUA data on average salaries by type of institution.

Staff experience, certification, and turnover. GAIN respondents were asked to estimate the average years of experience for all professional audit department staff. These data are shown in Table 7 on the following page; on average, the internal audit staff at ACUA member institutions are highly experienced.

The GAIN questionnaire also asked a number of questions about staff certifica-

Continued on page 23

Chart 1

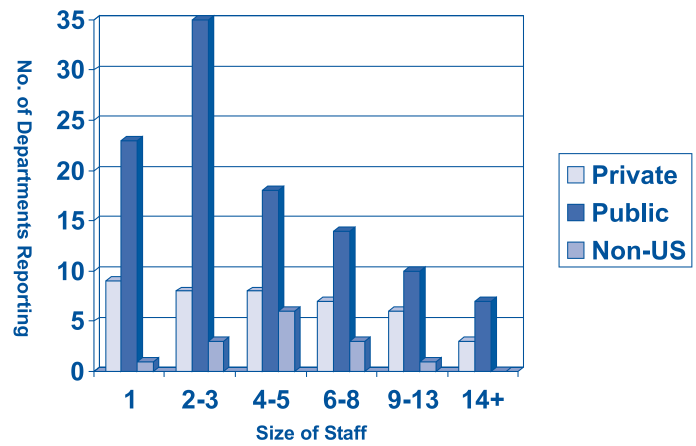


Table 5

Institution Type	Costs per Prof FTE
Private	$89,243
Public	$69,255
Non-US	$61,324

Table 6

Institution Type	Position	Average High Salary	Average Med Salary	Average Low Salary
Private	Director/CAE	$105,005	$90,304	$76,855
	Supervisor	$65,217	$59,845	$53,522
	Staff Auditor	$51,190	$44,878	$39,878
	Admin/Clerical	$34,462	$30,929	$28,845
Public	Director/CAE	$76,931	$73,785	$67,994
	Supervisor	$57,181	$53,654	$49,042
	Staff Auditor	$47,113	$43,324	$38,451
	Admin/Clerical	$30,332	$28,524	$28,058
Non-US	Director/CAE	$82,717	$73,810	$64,771
	Supervisor	$51,104	$41,868	$40,368
	Staff Auditor	$32,533	$23,376	$22,432
	Admin/Clerical	$19,841	$15,885	$13,774

Continued from page 22

tion and turnover. The results from these questions are summarized in Table 8 on the following page.

Reporting relationship. The final two tables in this summary present information on the reporting relationship of respondent audit departments. Table 9 below shows the administrative relationship (i.e., who approves the department's budget requests, performs the CAE's performance reviews, etc.).

Table 10 below shows the functional relationship (i.e., who is responsible for policy and general oversight).

It may be seen that the majority of private departments report administratively to the CFO and functionally to the Audit Committee, while for public departments, the majority report administratively and functionally to the President and CEO.

Next *CandU Auditor* Article

The next issue of *CandU Auditor* will present a summary of the ABACUS GAIN 2002 data on customer satisfaction, Chief Auditing Executive characteristics, annual and long range planning, activities audited, audit life cycle and resources, IT auditing, successful auditing practices, and continuous improvement. The issue after that will explore the similarities and differences between the practice of internal auditing in higher education and in other industries, using the 2002 GAIN data for comparison.

ABACUS GAIN 2002 Data Available for Additional Secondary Analyses

The ABACUS GAIN 2002 data, minus name of institution, are available for secondary benchmarking analyses by any ACUA member institution, upon request to the Chair of the Best Practices Committee.[2] Requests will be honored for any subset of institutions numbering over 10, which is the minimum group size imposed by the ACUA Board to maintain anonymity.

Notes

1. ACUA members who wish to get a copy of the 1999 comprehensive survey report may do so by contacting the ACUA office. The 2000 best practices report remains available on the University of Florida Web site at http://oig.ufl.edu/abacus/reports.html
2. Currently Steve Jung, e-mail sjung@leland.stanford.edu, or 650-725-0076.

Table 7

Institution Type	Average Yrs Exp Internal Auditing	Average Yrs Exp Public Accounting	Average Annual Exp Other	Average Yrs Total Yrs Experience
Private	9.1	3.1	5.8	17.7
Public	10.4	2.4	6.4	17.6
Non-US	8.4	4.4	5.5	18.2

Table 8

Institution Type	Average % of Staff Positions Turning Over in One Year	Average % of Staff with 1 or More Prof Certification
Private	25.2%	69.7%
Public	19.6%	78.7%
Non-US	18.7%	61.2%

Table 9

Institution Type	Audit Committee	CEO	President	CFO	Controller	Other
Private	0.0%	11.9%	11.9%	54.8%	0.0%	21.4%
Public	2.8%	10.3%	45.8%	27.1%	1.9%	12.1%
Non-US	0.0%	17.6%	23.5%	23.5%	0.0%	35.3%

Table 10

Institution Type	Audit Committee	CEO	President	CFO	Controller	Other
Private	53.5%	2.3%	0.0%	34.9%	0.0%	9.3%
Public	23.8%	10.5%	42.9%	12.4%	1.0%	9.5%
Non-US	69.2%	7.7%	15.4%	7.7%	0.0%	0.0%

IIA CQIA & Caltech

By Rick Moyer, California Institute of Technology

The California Institute of Technology (Caltech) prides itself on being one of the world's top institutes of research and instruction in science and engineering. Caltech faculty members repeatedly receive prestigious awards and currently include four Nobel laureates. In keeping with this standard of excellence, Audit Services and Institute Compliance (ASIC), a quality-focused part of the Caltech family, recently earned The Institute of Internal Auditors (IIA) Commitment to Quality Improvement Award (CQIA).

The Institute

An independent, privately supported institute in Pasadena, California, Caltech, which received more than $1.6 billion in grants and contracts in 2002, includes the Jet Propulsion Laboratory (JPL), Palomar Observatory and the W.M. Keck Observatory. Caltech has a student body of approximately 900 undergraduates and 1,100 graduate students.

JPL is the National Aeronautics and Space Administration's lead center for robotic exploration of the solar system, with JPL spacecraft having visited all planets in our solar system except Pluto. JPL telescopes observe distant galaxies to study how our solar system was formed, and the Deep Space Network communicates with spacecraft and conducts scientific investigations. JPL cameras and sensors study the ozone, oceans and other Earth sciences. JPL's budget in 2002 was approximately $1.4 billion.

Audit Services and Institute Compliance

In 2000, the internal audit department at Caltech was reestablished as ASIC. With the strong support of senior management and the Board of Trustees Audit Committee, the organization has undergone a complete transformation since 2000.

ASIC today is composed of 13 audit and compliance professionals, only one of whom was here in 2000. The first major step toward earning the IIA Commitment to Quality Improvement Award was recruiting a talented team possessing the knowledge, skills and disciplines needed to carry out our responsibilities. Because of the diversified nature of Caltech, ASIC employed a staff with varied backgrounds. The management team has two members with aerospace backgrounds, one of whom also has an environment, safety and health background; one member with a strong IT background; one member with a public accounting background; and another member with a diversified background in audit and consulting, including several years in higher education. The average experience level of the team is 19 years.

Once the new management team was in place, a new charter, vision and mission were developed. The charter describes a commitment to comply with the IIA's Code of Ethics and Standards for the Professional Practice of Internal Auditing. It also describes the mission, commitment, authority, independence, accountability and the audit and compliance services provided.

ASIC's mission is to proactively partner with management, faculty and staff to ensure that the campus, JPL and other Caltech operations effectively:

- Identify and manage risks;
- Comply with applicable laws, regulations, agreements and internal procedures;
- Maintain financial and operational integrity;
- Establish and maintain an appropriate control environment, level of accountability and ethical framework; and
- Monitor and improve processes.

The ASIC vision is to be a valued partner and advisor to management, faculty and the Audit Committee of the Board of Trustees.

Commitment to Quality Improvement Award

In 1999, The Institute of Internal Auditors established the CQIA as a semiannual recognition program. This prestigious international award recognizes internal audit activities for what

Continued on page 25

Continued from page 24

they have achieved to date, as well as for their commitment to continued improvement. The award recognizes professional excellence, quality of service and professional outreach.

Professional Excellence

The internal audit staff must possess the knowledge, skills and disciplines needed to carry out its responsibilities. ASIC was evaluated on certifications and professional designations, continuing professional education and signed audit reports. Currently, over three-fourths of the staff possess an advanced degree or professional certification. The remainder are actively pursuing the same. The diversity of the staff is also evident in the variety of certifications held, including: Certified Internal Auditor (CIA), Certified Public Accountant (CPA), Certified Fraud Examiner (CFE), Certified Information Systems Auditor (CISA), Certified Government Auditing Professional (CGAP) and Certified Professional Environmental Auditor (CPEA). A CIA signs all audit reports.

To demonstrate our commitment to continuing professional development, each staff member attends a minimum of 40 hours of training and development annually. In addition to attending ACUA and IIA conferences and seminars, members attend numerous research compliance training sessions sponsored by Caltech's Office of Sponsored Research. ASIC also sponsored a three-day ACL class at Caltech for the entire staff, as well as classes on the PricewaterhouseCoopers TeamMate audit management system and on time management. Additionally the director and one manager attended the "Effective Compliance Programs in Higher Education" workshop hosted by the University of Texas System.

Quality of Service

The internal audit department must demonstrate a commitment to carry out its mission within the organization. ASIC was evaluated on a department charter, customer satisfaction surveys, quality initiatives, benchmarking and quality assurance reviews. When the charter was updated, it clearly documented our unwavering commitment to proactively partner with and support Caltech management's efforts to ensure a solid control environment and an effective compliance program. The Audit Committee chairman, the Caltech president and the ASIC director approved the charter. To ensure that ASIC was providing a valuable service to its customers, the use of Customer Satisfaction Surveys after the completion of audit and compliance projects was recently implemented. By participating in the IIA's Global Auditing Information Network (GAIN) survey, ASIC was able to benchmark its services. An external peer review within the past three years helped launch the initial effort to establish ASIC. Another peer review is planned for 2003/04.

***Front row**, l to r, Rick Moyer, Charles Cotillier, Tye Welch, Rhoda Chang, Lynn Theriault, Nancy Narasaki, Helga Elsesser, Kathi Snodgrass, Pam Koyzis, Ed Shapiro, and Jon Bek. **Second row**, l to r, Carmen Ferguson, Kevin Caporicci, Susan Mantikas, and Mark Canevari.*

Professional Outreach

Members of the department must make measurable contributions to the profession of internal auditing. ASIC was evaluated on membership in the IIA, participation in IIA meetings, leadership in the IIA and other professional activities. ASIC has a group membership in the IIA. Three ASIC members are currently active in IIA leadership and meetings. The director is a member of the IIA International Committee for Professional Conferences and previously served as the chairman of the IIA International Committee on Academic Relations, a member of the IIA Research Foundation and a past president of the San Diego Chapter of the IIA. Another team member serves on the Board of the San Fernando Valley IIA Chapter and is a past president of the Beach Cities chapter. Another team member is the chairperson of the Awards committee for the San Fernando Valley IIA chapter. Finally, another member is an assistant professor at California State University, Los Angeles, teaching accounting and auditing courses.

Award Receipt

We received our award in early 2003 for the year 2002. Only 22 other audit organizations received this award in 2002. Only one other audit organization from higher education, Oak Ridge Associated Universities, has received the award since its inception in 1999. Letters acknowledging our award were sent by the IIA to the Caltech president, Audit Committee chairman and vice president for business and finance. A plaque was presented at the San Fernando Valley IIA Chapter meeting in March 2003, and ASIC was recognized and commended for receiving the award at the April 2003 Caltech Audit Committee meeting. Additional information about the award is available at the IIA Web site under Services/Quality Assurance Reviews/Commitment to Quality Improvement.

Our Ongoing Commitment and Challenge

We are very much committed to excellence in all that we do to support Caltech. The pursuit and receipt of this award challenge us to ensure that we continue to meet the highest professional standards. Although we are proud to have received this award, we recognize the need for continued improvement to be a valued partner and advisor at Caltech. We strongly encourage other audit organizations in higher education to pursue this award and demonstrate to management and Boards the quality of your organization.

About the Author

Rick Moyer is director of Audit Services and Institute Compliance at Caltech. You may contact him at rick.moyer@caltech.edu.

Association of College & University Auditors
342 North Main Street
W. Hartford, CT 06117-2507

PRSRT STD
U.S. POSTAGE
PAID
HARTFORD, CT
PERMIT NO. 2115

47th Annual Conference Highlights

Nashville
Pickin' the right path
Working in harmony

Sunday Reception and Exhibits – Networking at its best!

General Sessions – Featuring a return visit by Dr. Dale Henry for a motivational opening on Monday that promises to entertain as well as educate. On Tuesday, Dr. Michael Hoffman tackles issues surrounding ethics and leadership. Dr. Rick Whitfield opens the day on Wednesday with his keynote on higher education's changing risk environment and how senior university administrators are addressing it.

Educational Tracks – Running concurrently, there are seven or eight sessions to choose from for a total of 62 educational choices. With so many great topics presented by some of our best speakers, there is something for everyone.

Daily Networking – The networking isn't over on Sunday. ACUA attendees meet for breakfast every morning, lunch on Monday and Wednesday, and dinner on Wednesday night. Wait! It's not just dinner on Wednesday night, it's entertainment ACUA style! See page 1 of the conference brochure for details.

Optional Tours – While in Nashville, take advantage of the tours designed to acquaint you with the area. The tours are conducted for our members so even if you're at the conference by yourself, you'll be seeing Nashville with your ACUA colleagues.

For more details, go to www.acua.org. If you still have questions, call headquarters at (860) 586-7561 or send e-mail to acua@acua.org.

See you in Nashville, September 14-18, where we'll be *Pickin' the Right Path...Working in Harmony.*