Looking Forward to a Great Chapter Year!

Thank you for all your continued help and support over the 2014-2015 Chapter Year. We’ve had a great deal of help from our members and friends of the Chapter this last year.

Upcoming Training Events
We are looking forward to another great year for the Spokane Chapter of the IIA. As our goal this upcoming year is to continue to add value to the internal audit profession here in the Spokane area, we have already started the task of planning training activities that add value to our Chapter members. We would like to select topics of interest to you as well, so we ask for your input in identifying pertinent training topics (ideally, those which attract auditors across the various industries represented in our Chapter). Please contact a member of the 2015-2016 Chapter Board with any training ideas you have for this next year, and stay tuned for additional communications on upcoming events.

Articles in this Edition
I’ve included a couple articles of interest in this month’s newsletter. See the “IT Audit Corner” for a recent GAO report, which reports that financial regulators are not doing enough to analyze cyber risk across our organizations (are we?). I’ve also included an article on civility in our work in the “Back to Basics” section. I truly believe that maintaining civility with our auditees will help us, them, and our organizations as a whole. Civility is the first sign of respect, which we hope to earn with our auditees.

Open Job Opportunities
Also included with this newsletter are three current job opportunities located in our area. We pass these along as a service to our members.

Have a great month, and Happy Auditing!

Best Regards,

Stephen Hunt, CIA
Spokane IIA Board of Governors
Banking regulators are not adequately analyzing risks across institutions' enterprises, and not all IT examiners are well trained, according to a new report from the Government Accountability Office (GAO) about cybersecurity within the U.S. banking industry.

But a new GAO report also notes that not all regulatory agencies have the same oversight authority. In its report, "Cyber Security: Bank and Other Depository Regulators Need Better Data Analytics and Depository Institutions Want More Usable Threat Information," the GAO calls on Congress to take action to address this imbalance.

"Bank regulators directly address the risks posed to their regulated institutions from third-party technology service providers, but the National Credit Union Administration lacks this authority," the GAO notes. "Cyber-risks affecting a depository institution can arise from weaknesses in the security practices of third parties that process information or provide other IT services to the institution. Bank regulators routinely conduct examinations of service providers' information security. Authorizing NCUA to routinely conduct such examinations could help it better ensure that the service providers for credit unions also follow sound information security practices."

The Office of the Comptroller of the Currency, the Federal Deposit Insurance Corp., the Board of Governors of the Federal Reserve System and NCUA are all responsible for regulatory oversight and examination of depository institutions, and all are part of the Federal Financial Institutions Examination Council, which sets examination rules and guidelines.

All of these agencies, except for the NCUA, have the authority to conduct information security examinations of institutions' third-party service providers.

The Consumer Financial Protection Bureau also has authority to examine institutions with more than $10 billion in assets for compliance with consumer protection laws, but the GAO did not review the bureau's activities for the report.

**NCUA's Reaction**

NCUA Executive Director Mark Treichel says the agency agrees with the GAO that the credit union regulator should have authority to review third-party service providers for cybersecurity resilience.

"Parity among regulators of depository institutions in oversight authority vis-à-vis technology service providers would go far toward preventing third parties from transmitting material cyber risks to their clients," Treichel says.

And NCUA Chairwoman Debbie Matz notes in a statement about the report that this is not the first time that the GAO has recommended Congress grant third-party oversight authority to NCUA.
"In assessing current cybersecurity risks, GAO also references its 1999 and 2003 recommendations to provide NCUA with vendor authority," Matz says. "The 2003 assessment noted that third-party arrangements can help credit unions manage costs, provide expertise and improve services to credit union members, but they also present risks, such as threats to security systems, weakness of processing, availability and integrity of the systems."

Ben Hardaway, an NCUA spokesman, tells Information Security Media Group that the NCUA had temporary vendor examination authority from 1998 until 2001, as part of the nation’s response to Y2K.

"Vendor authority is NCUA's top legislative priority," Hardaway says. "Without vendor authority, NCUA cannot accurately assess the actual risk present in the credit union system, and whether current CUSO [Credit Union Service Organization] or third-party vendor risk-mitigation strategies are adequate and can effectively protect the system. The agency will continue to work with members of Congress to ensure the agency has the same legal authority that other federal financial institutions regulators have."

But Shirley Inscoe, a financial fraud expert and analyst for consultancy Aite, does not expect Congress to take action on the issue soon.

"I am surprised NCUA cannot examine third parties; since bank regulators can do so, it just makes sense that this body should be able to as well," she says. "It takes Congress a long time to get anything done, though, so I wouldn’t expect change to happen quickly."

Data Analytics
Beyond the NCUA’s third-party assessment inadequacies, the GAO also notes that banking regulators across the board are not routinely collecting all appropriate security incident data and documenting cybersecurity deficiencies during examinations. Examiners have also historically failed to classify deficiencies by category, which has made assessing an institution's overall cybersecurity challenging, the GAO finds.

"Regulators generally focused on IT systems at individual institutions, but most lacked readily available information on deficiencies across the banking system," the GAO states. "Having such data would better enable regulators to identify and analyze trends across institutions and use that analysis to better target areas for review at institutions."

Having that kind of information is critical, the GAO notes - a point with which regulatory agencies agree.

In his response to the GAO report, Comptroller of the Currency Thomas Curry says FFIEC agencies already are working to enhance cybersecurity data collection during their IT examinations through use of the new Cybersecurity Assessment Tool.

"This tool will provide the OCC with a repeatable and measurable process for assessing both the level of risk and the maturity of risk management processes within and across OCC-supervised institutions," Curry says. "This data will allow the OCC to monitor industry trends and identify new or emerging weaknesses where additional guidance or supervisory actions may be needed."
Better Examiner Training

Curry says this assessment tool also will provide data that regulatory agencies can use to help them better ensure all IT examiners are adequately trained - another cybersecurity shortcoming the GAO notes.

The GAO says most of the country's largest institutions are usually examined by IT experts. However, mid-sized and smaller institutions are at times reviewed by examiners with little or no IT training, according to the watchdog agency.

"The regulators recognized that some IT training is necessary for all examiners, so each regulator had efforts under way to increase the number of their staff with IT expertise and conduct more training," the report notes.

Curry says the assessment tool will enable regulators to identify and target training needs for examiners, especially those who work with smaller institutions.

"We expect to begin using the Cybersecurity Assessment Tool in selected examinations that commence during the fourth quarter of 2015," he says.

Read the original article HERE.
We hope you’ve enjoyed our 2014-2015 Chapter Year events! As you can see from our calendar below, we are currently looking for training ideas, but this calendar will fill up fast! Please email us to let us know if you have any topics you’d like to see over this next Chapter Year. See you at our first event this September!

### Spokane Chapter - Institute of Internal Auditors

#### 2015 – 2016 Chapter Year

<table>
<thead>
<tr>
<th>SEPTEMBER</th>
<th>OCTOBER</th>
<th>NOVEMBER</th>
<th>DECEMBER</th>
</tr>
</thead>
<tbody>
<tr>
<td>TBD</td>
<td>TBD</td>
<td>TBD</td>
<td>TBD</td>
</tr>
<tr>
<td>TBD CPEs</td>
<td>TBD CPEs</td>
<td>TBD CPEs</td>
<td>TBD CPEs</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>JANUARY</th>
<th>FEBRUARY</th>
<th>MARCH</th>
<th>APRIL</th>
</tr>
</thead>
<tbody>
<tr>
<td>TBD</td>
<td>TBD</td>
<td>TBD</td>
<td>TBD</td>
</tr>
<tr>
<td>TBD CPEs</td>
<td>TBD CPEs</td>
<td>TBD CPEs</td>
<td>TBD CPEs</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>MAY</th>
<th>JUNE</th>
<th>JULY</th>
<th>AUGUST</th>
</tr>
</thead>
<tbody>
<tr>
<td>TBD</td>
<td>No scheduled events</td>
<td>No scheduled events</td>
<td>No scheduled events</td>
</tr>
</tbody>
</table>

Check next month’s newsletter for training information!!
Open Job Opportunities

**Position Title:** Auditor

**Job Description:** Perform risk assessments, control evaluation, testing, drafting and communicating findings and reports to management. You can evaluate the effectiveness of operational, financial, and technological controls, as well as compliance and risk management processes, and various governance and management activities designed to ensure that business objectives are achieved and risks effectively managed. Our goal is to provide senior management and the Board of Directors with the best possible information with which to make risk-informed decisions. You can prepare opinions of findings and recommendations. Demonstrate compliance with all bank regulations for assigned job function and applies to designated job responsibilities – knowledge may be gained through coursework and on-the-job training. Work independently under general supervision with moderate latitude for initiative and independent judgment. Ensure assignments are completed both within budget and with high quality. Keep up to date on regulation changes.

**Education / Certification Requirements:**
- 3-5 years of experience with bank operations, bank regulatory compliance, audit, and/or SOX
- BA/BS preferably in Accounting, Business, or Economics
- CPA, CIA, CISA, CFE or CRCM preferred

---

**Position Title:** Senior IT Auditor

**Job Description:** Duties include performing IT risk assessments; planning, leading, and performing audit engagements; documenting work in conformance with auditing professional standards; developing audit issues and drafting reports; and presenting findings to the Chief Auditor and respective Bank management stakeholders. The position offers the opportunity to leverage and expand your auditing, risk management, and technical skills in a number of critical areas of contemporary auditing and banking, including: CAATs and audit data analytics; integrated auditing; Governance Risk and Compliance (GRC); data quality management and governance; Dodd-Frank Stress Testing (DFAST); and cybersecurity risk.

**Education / Certification Requirements:**
- 5+ years of IT/IS or operational audit, information security, or IT risk management experience
- Knowledge of CAATs tools and techniques
- CISA, CIA, CISSP, CAMS, SSCP, CISM, GIAC, PMP or other professional or industry related designations highly desirable
- Should have working knowledge of common IT and operational risk and control frameworks (e.g. COBIT, COSO, ITIL, etc.)
- Understanding of Sarbanes-Oxley (SOX), including risk assessment, IT general controls design and effectiveness testing, and SOX reporting requirements
Position Title: Auditor 2 – Internal Auditor

Job Description: Plan, conduct and/or lead moderately complex operational, compliance, IT and financial audits of various departments, branches and/or processes within the company in accordance with department and professional standards. Complete and/or oversee the completion of audit procedures; draft concise and accurate audit reports; and present findings and recommendations for corrective actions to management.

Education / Certification Requirements:
- Bachelor’s Degree in related field or an equivalent combination of work experience and education.
- CIA, CBA, CFSA, CISA OR CPA preferred.

Back to Basics

Sometimes it’s good to get back to the basics of something we do every day. In this section of the newsletter we will review some of the basic skills and practices that internal auditors use on a daily basis.

The Power of Civility

By: Carolyn Saint, CIA, CRMA, CPA, Chief Audit Executive, University of Virginia

The Idea: I had the good fortune to be invited to an Open Compliance and Ethics Group (OCEG) Leadership Council last year. We were treated to a presentation by Dr. Christine Pearson, Professor of Global Leadership at Thunderbird University, called “The Power of Civility.” Every participant at the Council remarked on it as one of the high points of the event and its impact on me has endured ever since.

The Execution: Dr. Pearson’s research shows that incivility causes high, unaccounted for costs. The corollary to that is improved civility increases productivity, commitment, retention, satisfaction/happiness, creativity, cooperation, and health. Increasing civility is a good business idea. But what does incivility mean and what can we do to decrease it?

Dr. Pearson’s definition of incivility: Seemingly inconsequential, inconsiderate words and deeds employee-to-employee. Lack of mutual respect among employees.

What does incivility look like?

- Taking too much credit for collaborative work.
- Keeping people waiting needlessly for appointments.
- Talking down to others.
- Delaying access to information or resources.
- Acting irritated when someone asks for your help.
- Dismissing/ignoring others’ ideas.
- Spreading rumors about colleagues.
• Grabbing the best assignments; leaving the worst.
• Hibernating in e-gadgets or emailing/texting during meetings.

It seems to me that internal auditors are often the target of incivility in the workplace based on the nature of our work. It’s often okay to roll one’s eyes and joke in various ways about “the auditors,” and we’ve all experienced push back on our need for documentation, meetings, or access to information. It can feel personal. A thick skin is a job requirement, yet we’re human. Being human, it’s sometimes enticing to counter incivility with … more incivility. There’s a momentary pleasure in giving back what’s being dished out. But at what cost?

Dr. Pearson’s research quantified the impact of incivility and the numbers are sobering:

• 47 percent cut back time at work.
• 63 percent lose work time worrying about their offender.
• 66 percent cut back effort at work.
• 78 percent say their commitment to their organization declines.
• Half consider leaving.
• 1 in 8 actually leaves:
  o Taking knowledge, networks, and experience (they’ll report a different reason).
  o Often after waiting months or years, so there is a time lag between incivility and exit.
• 88 percent get even with their organizations (fraud risk, internal auditors!).
• 94 percent get even with their offenders.
• … and these numbers regard targets of incivility only, rather than “innocent bystanders.”
• Costs can easily be in the millions.

What’s Dr. Pearson’s prescription for you to take ASAP? What to do personally? “Ooze civility.”

• Listen better.
• Smile more.
• Sincerely say please, thank you, excuse me, I’m sorry.
• Think before you speak.
• Seek feedback. Make sure you’re civil.
• Practice the 10/5 rule (eye contact at 10 ft.; verbal greeting at 5 ft.)
• Extend yourself, especially to people who tend to be ignored.
• Drop arrogance. Appreciate why humility rules.
• Admit when you don’t know.
• Share recognition/praise (high performing teams get 6 times as much positive feedback; low performing teams receive 2 times more negative feedback).
• Be generous, including time.
• Hire with vigilance. Don’t let uncivil people in your door.
• Live up to your organization’s values.

Will increasing our civility help our stakeholders see us as trusted advisers? Perhaps. Will it make you feel good as an auditor and a person? Absolutely. See if you can fill this prescription starting today. Doctor’s orders!

This article comes from the IIA Internal Auditor blogs at https://iaonline.theiia.org/. See the original article at https://iaonline.theiia.org/the-power-of-civility.
2015 – 2016 IIA Spokane Chapter Officers

Spokane IIA Chapter Officers elected for the 2014-2015 Chapter Year:

<table>
<thead>
<tr>
<th>Title</th>
<th>Officer</th>
<th>Organization</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chapter President</td>
<td>Vanessa Scarpelli</td>
<td>Umpqua Bank</td>
</tr>
<tr>
<td>VP Membership</td>
<td>Melanie Shanks</td>
<td>Spokane Teacher’s Credit Union</td>
</tr>
<tr>
<td>VP Programs</td>
<td>Lisa Michalski</td>
<td>Umpqua Bank</td>
</tr>
<tr>
<td>VP Communications</td>
<td>Marie Rice</td>
<td>Management Consultant</td>
</tr>
<tr>
<td>Treasurer</td>
<td>Terra Kile</td>
<td>dm-t</td>
</tr>
<tr>
<td>Secretary</td>
<td>Lisa Sanborn</td>
<td>Numerica Credit Union</td>
</tr>
</tbody>
</table>

2015 – 2016 IIA Spokane Chapter Board of Governors

Spokane IIA Chapter Board of Governors for the 2015-2016 Chapter Year:

<table>
<thead>
<tr>
<th>Governor</th>
<th>Organization</th>
</tr>
</thead>
<tbody>
<tr>
<td>Penny Brown</td>
<td>AmericanWest Bank</td>
</tr>
<tr>
<td>Stephen Hunt</td>
<td>AmericanWest Bank</td>
</tr>
<tr>
<td>Debra Peterson</td>
<td>Washington Trust Bank</td>
</tr>
<tr>
<td>Cathy Cook</td>
<td>Washington Trust Bank</td>
</tr>
<tr>
<td>David Gifford</td>
<td>Washington Trust Bank</td>
</tr>
<tr>
<td>Dawn Flerchinger</td>
<td>Clearwater Paper</td>
</tr>
<tr>
<td>Colleen Warner</td>
<td>Global Credit Union</td>
</tr>
</tbody>
</table>

Click here to opt-out of future communications from the IIA Spokane Chapter.