The SANS Institute was established in 1989 as a cooperative research and education organization. Its programs now reach more than 165,000 security professionals around the world. At the heart of SANS are the many security practitioners in various global organizations, from corporations to universities, working together to help the entire information security community.

While technical training is of paramount importance, SANS also recognizes that non-technical individuals need training on awareness and compliance if information security is to be achieved across an entire organization. Therefore, SANS Securing The Human was created to provide computer based training for the end user. The training product line has since expanded to serve end users, developers, ICS engineers, utilities, and the healthcare market. We also now offer phishing testing as a complement to our current portfolio of security awareness products.

It is our mission to provide you with training and testing tools to ensure you meet compliance requirements while changing human behaviors and reducing risk.

---

**IT Audit Corner**

**Passwords**

**Background**

Passwords are one of the primary ways we prove who we are. It is how you access your email, bank online, purchase goods and access devices such as your laptop or smartphone. In many ways, passwords are the keys to your kingdom. As a result, if someone has your password, they can steal your identity, transfer your money or access all of your personal information. Strong passwords are essential to protecting your identity and information. Let’s learn what makes a strong password and how to use them securely.

**Strong Passwords: Passphrases**

The problem is cyber criminals have developed sophisticated programs that can guess, or “brute force,” your passwords, and they are constantly getting better at it. This means they can steal your passwords if they are weak or easy to guess. Never use common information for your passwords, such as your birth date, your pet’s name or anything else that can be easily determined from your social networking posts or Google. Instead, the best way to create a strong password is to use a long password, and the more characters you have, the better. In fact, instead of using a single word, use multiple words -- or even a complete sentence. This type of password is called a passphrase, and it is one of the strongest you can use. Here is an example of one:

*time for my coffee*

That is it; that is all you need. If required, you can make your password even stronger by adding symbols, capital letters or numbers, such as those you see in the example below. This is especially important if you are using a website that does not allow multiple words or a complete sentence for your password:

*Time f0r my coffee!*

---

**Auditor's Corner**

**The Power of Observation**

As auditors, we often rely on our powers of observation to detect issues and assess risks. Observation can be a powerful tool, allowing us to gather information indirectly and get a sense of what is happening in an organization. However, it is crucial to remember that observation alone may not always provide a complete picture.

For example, when we observe a system for the first time, we may notice a particular process that is not following proper procedures. However, to truly understand the issue, we need to dig deeper. We might ask questions to explore why the process is being performed in that way, or we could conduct a test to see if the process is actually working as intended.

In this case, observation helped us identify a potential risk, but further investigation was necessary to fully understand the situation. This highlights the importance of combining observation with other audit techniques, such as interviewing personnel or reviewing documentation, to ensure a comprehensive assessment.

---

**Audit Tips**

**Effectiveness of Electronic Signature Systems**

Electronic Signature Systems (ESS) have become increasingly popular in recent years. However, it is important to evaluate their effectiveness to ensure they are being used correctly and securely.

To do this, auditors should consider the following:

1. **Purpose and Scope:** Define the purpose and scope of the ESS and ensure it aligns with the organization’s objectives.
2. **Creation of电子签名:** Ensure that the electronic signatures are created and managed properly. This includes verifying the identity of the signer and ensuring the signature is not altered.
3. **Audit Trails:** Maintain detailed audit trails that capture the history of electronic signatures, including who signed what and when.
4. **Security Measures:** Evaluate the security measures in place to protect electronic signatures, such as encryption and user authentication.
5. **Compliance:** Confirm that the ESS is compliant with legal and regulatory requirements.

By following these steps, auditors can assess the effectiveness of ESS and recommend improvements if necessary.
Notice how this example uses a capital letter. You can also replace letters with numbers or symbols, such as replacing the letter ‘a’ with the ‘@’ symbol and the letter ‘o’ with the number zero, or use common punctuation marks such as a question mark, period or even spaces. If a website or program limits the number of characters you can use in a password, use the maximum number of characters allowed.

**Using Passwords Securely**

In addition to using strong passwords, you must be careful how you use them. Having a strong password is no good if bad guys can easily steal or copy it.

1. Be sure to use different passwords for different accounts. For example, never use the passwords for your work or bank accounts as the passwords for your personal accounts, such as Facebook, YouTube or Twitter. This way, if one of your passwords is hacked, the other accounts are still safe. If you have too many passwords to remember, consider using a password manager. This is a special program you run on your computer or mobile device that securely stores all of your passwords for you. The only passwords you need to remember are the ones to your computer and the password manager program. If your passwords are for work, then check with your supervisor or your help desk to see if using a password manager is permitted in your organization.

2. Never share your password with anyone else, including co-workers. Remember, your password is a secret; if anyone else knows your password it is no longer secure. If you accidently share your password with someone else or believe it may have been compromised or stolen, be sure to change it immediately.

3. Do not use public computers, such as those at hotels or libraries, to log into a work or bank account. Since anyone can use these computers, they may be infected with malicious code that captures all of your keystrokes. Only log in to your work or bank accounts on trusted computers or mobile devices you control.

4. Be careful of websites that require you to answer personal questions. These questions are used if you forget your password and need to reset it. The problem is the answers to these questions can often be found on the Internet, or even your Facebook page. Make sure that if you answer personal questions you only use information that is not publicly available or fictitious information you have made up. Password managers can help with this, as many allow you to store this additional information.

5. Many online accounts offer something called two-factor authentication, or two-step verification. This is where you need more than just your password to log in, such as codes sent to your smartphone. This option is much more secure than just a password by itself. Whenever possible, always use these stronger methods of authentication.

6. Mobile devices often require a PIN to protect access to them. Remember that a PIN is nothing more than another password. The longer your PIN is, the more secure it is. In fact, many mobile devices will allow you to change your PIN number to an actual password.

7. Finally, if you are no longer using an account, be sure to close, delete or disable it.
Upcoming Training Opportunities

Chapter Luncheons

FEBRUARY 2015
MANAGING COMPLIANCE RISK WITH THIRD-PARTY VENDORS

February 19, 2015
11:30 AM to 2:00 PM
Spokane Teacher’s Credit Union

Most organizations utilize third party vendors for everything from mailing advertising and invoices to outsourcing entire service and product lines from the initial sale to the final payment. But how well do organizations manage risk related to third party services? This presentation focuses on best practices in managing third party service providers and vendors and key practices and considerations internal auditors should consider when evaluating Company management practices over these vital service partners.

Dan Huston, CPA, CFIRS
PARTNER
MOSS ADAMS, LLP

Dan has worked in the banking industry since 1979 and has extensive knowledge of bank operations, lending, and related compliance. His focus is compliance with federal regulations, product development, and processing efficiency. Dan directs the firm’s internal audit and regulatory compliance services for financial institutions. Dan’s areas of expertise include credit underwriting and lending compliance, anti-money laundering program administration, item processing, funds delivery, fiduciary services, loan origination and servicing, and trust and fiduciary operations.

MARCH 2015
COSO 2013

March 11, 2015
11:30 AM to 2:00 PM
AmericanWest Bank

Colin Wallace
DIRECTOR – INTERNAL AUDIT AND ADVISORY SERVICES
MOSS ADAMS, LLP

APRIL 2015
PROFESSIONAL SKEPTICISM

STAY TUNED FOR ADDITIONAL DETAILS.
# Schedule of Events

## Spokane Chapter - Institute of Internal Auditors

### 2014 – 2015 Chapter Year

<table>
<thead>
<tr>
<th>Month</th>
<th>Date</th>
<th>Event Description</th>
<th>CPEs</th>
</tr>
</thead>
<tbody>
<tr>
<td>SEPTEMBER</td>
<td>Tuesday, 23rd</td>
<td>Excel: Intro to Macros</td>
<td>1 CPE</td>
</tr>
<tr>
<td>OCTOBER</td>
<td>Tuesday, 28th</td>
<td>IT Risk – Keeping Your Business Off the Front Page of the Newspaper</td>
<td>1 CPE</td>
</tr>
<tr>
<td>NOVEMBER</td>
<td></td>
<td>CANCELLED in lieu of the Annual ACFE Fraud Conference</td>
<td></td>
</tr>
<tr>
<td>DECEMBER</td>
<td>Thursday, 18th</td>
<td>Joint Holiday Luncheon with the ACFE</td>
<td>2 CPEs</td>
</tr>
<tr>
<td>JANUARY</td>
<td>Thursday, 22nd</td>
<td>Cancelled</td>
<td></td>
</tr>
<tr>
<td>FEBRUARY</td>
<td>Thursday, 19th</td>
<td>Managing Compliance Risk with Third-Party Vendors</td>
<td>2 CPEs</td>
</tr>
<tr>
<td>MARCH</td>
<td>Wednesday, 11th</td>
<td>COSO 2013</td>
<td>2 CPEs</td>
</tr>
<tr>
<td>APRIL</td>
<td>Date TBD</td>
<td>Professional Skepticism</td>
<td>2 CPEs</td>
</tr>
<tr>
<td>MAY</td>
<td>Date TBD</td>
<td>TBD Seminar</td>
<td>8 CPEs</td>
</tr>
<tr>
<td>JUNE</td>
<td></td>
<td>No scheduled events</td>
<td></td>
</tr>
<tr>
<td>JULY</td>
<td></td>
<td>No scheduled events</td>
<td></td>
</tr>
<tr>
<td>AUGUST</td>
<td></td>
<td>No scheduled events</td>
<td></td>
</tr>
</tbody>
</table>
Certification Corner

Internal Auditor Magazine

Earn 3 CPE credits by reading Internal Auditor (Ia) magazine articles and answering questions about them here.

Other CPE Opportunities

Individuals can also earn CPE credits by giving presentations, writing exam questions, and more. Visit your individual CPE certification page (above) for details or see the administrative directive.

Member Spotlight

The IIA Spokane Chapter will be spotlighting various chapter members each month to find out why the member chose their profession, what they do for fun (besides audit), and what has made them successful.

Member: Kortney Todd  
Position: Director of Internal Audit  
Company: Cashmere Valley Bank  
Certifications: CPA  
Education: Bachelor of Arts, Majors in Accounting & Finance  
Washington State University  
Graduated Cum Laude

Q: How did you become an internal auditor?

I started my career as a consultant specializing in business risk and internal audit at Protiviti. Protiviti allowed me the opportunity to work on non-audit projects which were very beneficial because these gave me the opportunity to learn about various business models and risk profiles. After Protiviti I joined Amazon’s internal audit department which re-focused my efforts solely on internal audit with some exposure to their benchmarking methodologies.

At Cashmere Valley Bank my main focus is internal audit but I am also involved in Enterprise Risk Management. I enjoy audit but I also enjoy challenges outside of the typical audit function. Thinking outside of the ‘audit mindset’ really allows me to learn about the entire business and the bank’s overall risk profile.

Q: What do you enjoy the most in your current position?

My team and the challenges of an ever-changing and evolving risk landscape. I enjoy change because it allows me the opportunity
to learn about new risks and new regulations and forces me to enhance my knowledge base.

**Q: What are some of the challenges you face in your current position?**

The ‘policeman badge mentality.’ I truly believe that audit can provide tangible value to an organization. If audit and management work cohesively the value to the organization increases significantly.

**Q: If you were not an auditor, what would you be doing?**

Furniture maker and world traveler.

**Q: What are your passions or hobbies outside of internal audit?**

Family, hiking, hunting, skiing, & watersports.

**Q: Any word of advice to fellow internal auditors?**

Companies don’t always recognize that Internal Audit can add meaningful value to their organization. Unfortunately, the majority of audit findings lead to extra work for the business units. It is rare, but there are situations where audit findings can lead to more efficient business processes. One of the ways that I have made this possible is by evaluating our system processes and outputs (management reports). Is the system functioning in a manner that allows the business unit to clearly understand the data? Can system parameters be altered in a way that allows the business to function more efficiently? These are questions that we should be asking ourselves during an audit. I consider audit findings that lead to more efficient business processes the best type of audit finding – one that benefits the company in a way that management truly understands!

---

**WANTED**

Volunteers to serve as
Institute of Internal Auditors Spokane Chapter Board members

We need you. Please contact David Gifford, Chapter President, if you or someone you know would do a great job of helping the chapter.
**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.

This month’s article comes from the ITauditSecurity blog.

**Top 10 Ways to be a Lovable Auditor**

A while back, I noted some reasons why people hate auditors. Well, you can hop those hurdles, and be an auditor that people love or at least respect. Here’s how:

1. Smile and use people’s names. Smiling says you’re a happy, pleasant person, who puts the interests of other first. Smiles put people at ease, and everyone loves the sound of his/her name – so use it often.

2. Keep your meetings short and focused, and publish an agenda before the meeting. Arrive at meetings early and be prepared (papers, projector, etc.). Occasionally bring good food.

3. When someone complains, ask questions to understand the complaint, the reason behind it, and how to fix it. Then fix it.

4. Ask auditees what you can do to make their jobs easier, then do it.

5. Avoid nitpickiness and aid understanding by continually asking yourself and your auditees, What’s the risk? If you can’t describe what could happen and the probability of it, think again. Keep the big picture in mind.

6. Never surprise an auditee with a finding; make sure you discuss it before you report it. This is fundamental, but some auditors still forget this.

7. Before you ask an auditee to explain a technical issue, Google it first. You may find your answer, have to only ask for minor explanation, or at worst, can ask a more intelligent question.

8. Listen more than you talk. When you do talk, be brief, explain what you need, and why.

9. Don’t ask for data or a person’s time before you need it. If you don’t really need something for a week, tell the auditee that.

10. Don’t audit departments during busy times (e.g., never audit payroll in January as it is running and sending W2 forms). Remember, audit serves the business, not the other way around.

11. Don’t throw your weight around. An auditor should always keep in mind that he/she is “here to help”.

12. Deliver more than you promise (in this case, more than 10 ways).

P.S. These tips even make security pros lovable too!
2014 – 2015 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>David Gifford</td>
<td>AmericanWest Bank</td>
</tr>
<tr>
<td>VP Membership &amp; Programs</td>
<td>Melanie Shanks</td>
<td>Spokane Teacher’s Credit Union</td>
</tr>
<tr>
<td>VP Communications</td>
<td>Stephen Hunt</td>
<td>AmericanWest Bank</td>
</tr>
<tr>
<td>Treasurer</td>
<td>Terra Kile</td>
<td>DeCoria Maichel and Teague P.S.</td>
</tr>
<tr>
<td>Secretary</td>
<td>Vanessa Scarpelli</td>
<td>Umpqua Bank</td>
</tr>
</tbody>
</table>

2014 – 2015 IIA Spokane Chapter Board of Governors

Spokane IIA Chapter Board of Governors for the 2014-2015 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>Debra Peterson</td>
<td>Washington Trust Bank</td>
</tr>
<tr>
<td>Cathy Cook</td>
<td>Washington Trust Bank</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.