



Kentuckiana ISACA Website

The purpose of this news letter is to provide a medium by which the Kentuckiana ISACA members can share auditing information, enable new members to establish a professional network, provide valuable career opportunities to members, and keep membership updated on the industry trends. Also available from your Kentuckiana ISACA group is our web-page that contains similar information in a dynamic and GUI format. If you have not seen our website, please check it out [here](#).

This award winning site contains chapter general information, career opportunities, past newsletters, contact information, reference material and more.

Next ISACA Lunch Meeting

Time: December 7, 2005

11:30 Check-in and Networking

12:00-1:00 Lunch and Presentation

CPE: 1 CPE Hour

Speaker - Topic:

David Gorgas – Information Security Governance: Aligning Security with Business to Produce Strategic Value and Effective Management Oversight

Speaker Bio:

Please see article on page 3.

Location:

[Vincenzo's](#) is located on South 5th Street in Downtown Louisville. Room A.

Menu Selections:

Tortellini

Land and Sea

Cobb Salad

RSVP: Carrie Ramsey by December 2, 2005.

Office: (502) 627-4738

Carrie.Ramsey@lgeenergy.com

Cost: \$20

Career Opportunities

The KY ISACA Chapter strongly believes in providing a medium through which members can network and grow professionally. To that end, the KY ISACA chapter offers a web page for job opportunities to our members and to the community. If you are interested in posting job opportunities on our website, please contact Michael Vincent for more information.

Current career opportunities posted are located on our [Louisville Area Job Openings Page](#).

Thank you for supporting the KY ISACA Chapter.

PayPal is a quick and simple way to pay for monthly IIA meetings. From the chapter web site (www.iialou.org), go to the meeting and seminar schedule page. Click the "pay now" button for the meeting you wish to pay for. If you already have a "PayPal" account, simply verify the amount; enter your log-in and password. *If you don't already have a "PayPal" account*, you will need to fill in the information for new members (similar to other ecommerce web sites such as Amazon). Once you have completed the transaction, you will be sent an e-mail receipt by PayPal and be returned to the Louisville IIA web site. The local chapter also receives an e-mail that tells us you have paid. You will **still need to contact Carrie Ramsey** with your menu choice. All information is exchanged via HTTPS protocol (secure and encrypted) and remains with PayPal.

PRESIDENT'S MESSAGE

From the desk of
Matthew Smith

Dear Members,

We had another very successful meeting in November with great member turnout. I'd like to thank Dr. Srinivasan again for his time and effort to present to us. We look forward to hearing from him in the future.

We have now completed our member survey and are in the process of reviewing and analyzing the results. In next month's newsletter, we will share some highlights from the survey after we have had an opportunity to aggregate the response data. The Kentuckiana Board thanks all those members who participated. Again, we value your feedback and we are committed to using the information we have gathered to add value for you in the future.

Our Chapter is currently making plans for a social event on January 19th, so mark your calendars now! Both Dr. Alan Lord from ISACA International and I will be speaking at this event, as well as giving you a chance to network with your peers in the Chapter. We are working hard to make this a very nice evening for you, so stay tuned for further details.

We are very fortunate to have David Gorgas from Humana speak at our next Chapter meeting on December 7th at Vincenzo's. The topic will be "Information Security Governance: Aligning Security with Business to Produce Strategic Value and Effective Management Oversight". I am really looking forward to hearing from David, as he is a former colleague and a friend of mine. I have learned a great deal from working with him, and I know you will too through his presentation to our group. So don't miss out on this opportunity to hear from a true professional. I hope to see you there.

Thank you and have a wonderful Thanksgiving holiday.

Regards,

Matthew Smith
Chapter President

Job Opportunity

Security Specialist

Do you have experience in information security? If so, Kentucky Farm Bureau Insurance may have the job for YOU! We are currently seeking an individual that will be responsible for working with the security manager to develop the overall strategy to control and protect information resources. This position will assist in evaluating and recommending security tools and technologies to help manage business risks and assist with the implantation of new security tools, technologies and procedures. Qualified applicants will possess the following:

- **Bachelor's degree preferred; CISSP, CISM or other security certification a plus!**
- **3+ years experience in information security required**
- **Experience with information security products including analysis, design implementation, maintenance, and support preferred**
- **Experience in Security Awareness training preferred**
- **Strong background in research and problem solving required**
- **Solid understanding of IT controls required**

We offer a competitive salary and an excellent benefits package.

Interested applicants MUST apply at www.kfbjobs.com.

Mailed and faxed resumes will not be reviewed.

Job ID # 1033

Equal Opportunity Employer

Biography of David Gorgas

David Gorgas is currently Manager of IT Security Risk and Compliance Management at Humana, Inc., a Fortune 200 health benefits company based in Louisville, KY. In his role at Humana David heads up Humana's IT Security Compliance and Risk Management programs. David is responsible for managing information risk against industry IT and Information Security best practices, and for managing IT and Information Security compliance with various compliance requirements, including Sarbanes-Oxley, HIPAA, GLBA, CMS, State Departments of Insurance, and Customer Group Contracts.

David has over 12 years' IT, IT Audit, and management experience in the financial services and health care industries, including key roles at Humana Inc., Trinity Health, Comerica Bank, and California Federal Bank. David graduated with a Bachelor of Arts Degree in Law Enforcement Administration from the University of Oklahoma and also attended graduated school at the University of Notre Dame. He holds the CISA and CIA certifications and also earned the CCNA certification in 2001.

David and his family live in Louisville, Kentucky, where his wife, Colette, works as a freelance artist with Recycled Paper Greetings. David and Colette have three sons (Jackson - 8, Hunter - 5, and Mitchell - 3) who are avid football fans and players. David and his whole family are huge Notre Dame fans.

Policy for Posting Positions:

There have been several inquiries from various parties regarding the KY Chapter of ISACA and posting job inquiries. Below are the requirements as outlined within KY ISACA Board meeting Minutes:

- Members
 - o Free in 1 month's newsletter
 - o Free for 30 days on KY ISACA website
 - o Member is responsible for renewing posting on a monthly basis
- Non-Members
 - o \$50 for 1 month's newsletter AND 30 days on KY ISACA website
 - o \$50 for each additional month

ISACA National News and Information

New Study Finds the Convergence of Traditional and Information Security Functions Necessary for Global Organizations to Protect Assets, Maintain Profits

Rolling Meadows, IL, USA (10 November 2005) – New threats and soaring costs are two factors driving the “convergence” or integration of traditional and information security functions in a growing number of U.S.-based global companies, according to the results of a new study commissioned by three leading international security organizations, ASIS International (ASIS), Information Systems Audit and Control Association (ISACA) and Information Systems Security Association (ISSA).

The study, [*Convergence of Enterprise Organizations*](#) (PDF, 1.5 MB), was conducted by Booz Allen Hamilton (BAH) and surveyed chief security officers (CSO), chief information security officers (CISO) and other security professionals representing 36 companies with revenues ranging from \$1 billion to more than \$100 billion. BAH also conducted 14 in-depth interviews in addition to the surveys. The results of the study indicate that convergence is a trend that impacts not just the security function of a given business, but rather, the business as a whole. Such integration ensures that all functions within the organization work together, and enables the organization to prevent, detect, respond to and recover from any type of security incident.

“In the society we live in today—with the threat of terrorism and a dramatic increase in the number and complexity of other security-related risks such as computer viruses, cyber attacks, theft, extortion and fraud—companies must find a more comprehensive approach to protecting their employees, core networks and facilities,” said Timothy L. Williams, CPP, Vice President of Corporate and Systems Security for Nortel Networks and a member of the ASIS Board of Directors. “Through the convergence model, security professionals have a unique opportunity to elevate their role in the organization, advance the security profession and deliver additional value to the organization through cost savings and related efficiencies.”

As new threats emerge and business transactions become more intricate, adhering to these regulations and compliance guidelines will also become more complex. Sarbanes-Oxley, for example, gives a framework under which risk must be assessed, but does not stipulate how to assess that risk. Business’ desire for security professionals who can examine and assess the risks that organizations face as a whole is one of the driving forces behind the convergence phenomenon, according to the study. The focus on security from an enterprise perspective has led to innovative approaches that emphasize integration—specifically, the integration of the risk side of business into the strategic planning side in a consistent and holistic manner.

Another factor identified in the study as contributing to the security convergence trend is the migration in the types of assets many organizations need to protect. Companies’ assets are now increasingly information-based and intangible, and even most physical assets rely heavily on information. Technology is also now allowing companies to offer more information products. As these products become increasingly intangible, there is a greater

need to integrate traditional and information security, as well as security throughout the entire enterprise.

“Organizations rely on their IT systems to provide real value, increase competitive advantage and improve relationships with customers and trading partners,” said Marios Damianides, CISA, CISM, CA, CPA, past international president of ISACA. “The convergence of logical and physical security is a natural progression that enables businesses to better protect all of their assets and achieve significant financial efficiencies.”

The advance of technology itself is blurring the line between traditional and information security, and is a third component driving convergence. Physical access control technology’s merge with network access technology is one example cited in the study. The *smart card* demonstrates a technology that is integrating once disparate parts of security, by verifying a person’s identity and tracking his or her physical location.

“Over the past year, we have seen a tremendous growth in the number of our members who are either partially or wholly responsible for both information and physical security,” said Dave Cullinane, president of the ISSA. “While this convergence is still only being embraced by a minority of the industry, it is clearly a road map for the future. Information exists in all forms, including the physical realm.”

As the convergence of security functions within organizations continues to increase, the study concludes that the role of security should no longer be viewed as a sunk cost, but rather, a value adding activity. So powerful and important is the integration of security functions within an organization, in fact, that the study predicts that companies embracing security convergence and facilitating its implementation will emerge as leaders not only in their own sectors, but across all sectors.

A webcast about the study will be available at the ASIS, ISACA and ISSA web sites in December. For more information or to download a free copy of [*Convergence of Enterprise Organizations*](#) (PDF, 1.5 MB), please visit the ASIS, ISACA or ISSA web site.

Note: This article is available in full at ISACA’s website at www.isaca.org. Please visit ISACA’s website for more articles and information on applying for CISA certification.

Forum

Risk Anemia

Basic financial analysis states that investments with no risk have minimal returns. It's a safe bet, but do not expect a wealthy return. On the flip side, huge risks have the potential for great returns, but the opportunity for failure exponentially increases as well. Thus exists the delicate balance within an organization to maintain healthy profits and minimize risks.

This delicate balance is commonly referred within the Enterprise Risk Management circles as the organization's risk appetite. Unfortunately, if you try to quantify this risk appetite, the city gates are assaulted with a plethora of no-nothing consultants bent on selling you snake oil solutions, heat maps, and visions of sugar plums dancing in your head.

Don't buy into the hype. Enterprise Risk Management has tremendous potential, but the current industry culture is simply not ready to embrace the concept fully. There are pockets of limited success, but the results are unfortunately somewhat underwhelming.

The major reason for this disinterest is for a variety of political, monetary, cultural, and economic reasons.

Politically, many senior executives would rather sell their soul to the devil than hand over the keys to their operational analysis to internal audit. The thought of having internal auditors monitoring their every move elicits Orwellian images. Senior executives are highly protective of their intellectual property, and very unwilling to let them go. This is understandable. I think many Chief Audit Executives would equally become disconcerted over the concept of having monitoring devices be placed around auditing metrics. It's creepy.

Monetarily, organizations may have a strong affinity towards risk. Specifically, small businesses especially enjoy risk and actively will pursue ventures that larger organizations would not touch with a ten foot pole. By placing risk constraints on an organization, you have effectively limited their ability to adapt to the changing market environment. Limiting risk alters the organization's business model. Why would a senior executive want limits on their ability to engage in ingenuity? Obviously there are limits that should not be crossed, but there is equally a case from the perspective of stockholders that a risk-anemic organization is equally irresponsible as a risk 'hyperphilic' organization such as

Enron. It is essential to remember that healthy organization must have risk. Unhealthy organizations accept too much, or too little risk.

Getting back to my original argument, this balance between risk anemia and risk obesity. It is the function of an internal auditor to make sure that the organization's overall strategic direction be taken into account when recommending risk based alterations to the organizations infrastructure. Failure to do so may result in confrontations with management that are unnecessary and unproductive.

Kentuckiana Chapter Officers**

Officer	Position	Company	email
Matthew Smith	President	YUM!	matthew.smith@yum.com
Bruce Edwards	VP & Web master	U of L	Bruce@quasarcomics.com
Michael Vincent	VP & Newsletter	Humana	mvincent@humana.com
Diane Kissel	VP Programming	Kindred Health Care	diane.kissel@kindredhealthcare.com
Bob Boyle	Treasurer	Strothman & Company	rboyle@strothman.com
Debbie Shelton	Past President, Secretary	LG&E Energy	Debbie.Shelton@lgeenergy.com
Carla Shields	Membership Director	Ajilon Finance	carla.shields@ajilonfinance.com
James Rose	Standards Liaison	Humana	jrose1@humana.com
Dave Barker	Academic Liaison	U of L	dfbark01@louisville.edu
Melissa Perry	CISA Coordinator		melissaperrycpa@yahoo.com
Danette Dillow	Asst. Treasurer	Republic Bank	DDillow@republicbank.com

Congratulations to those below who passed the CISA or CISM!

Mr. David Ryan Roling
Mr. Littlefield Matthew William, CISA,CPA
Mr. Michael Edward Kleopfel, CISA
Carolyn Fiske
Barry V. Scott, CISA
Lt.Col. Edward J. Maloney, III
Mr. Charles Raymond Snyder, PMP
Mr. Carl Lutes, CISA
Mr. Jeffrey Bradshaw
Mrs. Brogan Darla Jan, CISA
Mr. David Thomas Kozora, CISA
Brad Wolff
Mr. James E. Andriot, CPA, CIA
Mr. Richard Lee Taylor
Mrs. Carey Fansler
Mr. Phillip C. Forrest, ISO
Mr. Jeffrey O. Gercken, CISSP,CCNP,MCSE

Calendar of Events

ISACA

RSVP: carrie.ramsey@lqeenergy.com

Date / Location	Topic	Speaker
September 5 / Kindred Healthcare	IT Compliance for Dummies	Active Reasoning
November 2, 2005	Database Security & Control	Dr. S. Srinivasan
December 7, 2005 / Vincenzo's	Information Security Governance: Aligning Security with Business to Produce Strategic Value and Effective Management Oversight.	David Gorgas, CISA, CIA, CNNA
January 19, 2006 / TBD	Social Event	Dr. Alan Lord & Matthew Smith

Institute of Internal Auditors
RSVP: carrie.ramsey@lgeenergy.com

Date	Topic	Speaker
11/8/2005	ERM	James Rose, MA, CPA, CISSP
12/13/2005	Effective QARs	Jennifer Burke
1/10/2006 (AM)	Roundtable – Evolving Role of Internal Audit	Dave Barker
1/10/2006 (Lunch)	Evolving Role of Internal Audit	Teresa Snediger
2/2/2006 (All Day)	Fraud – 2006	Courtenay Thompson (& Associates)
2/14/2006	Alternative Dispute Resolution in Business	Tony Belak
3/14/2006	Quantitative Risk Assessment in Action	Bruce Edwards

