

December 2006

# Newsletter

---



## Inside This Issue

### Page

1	Table of Contents
2	Message to Membership
3	December Webinar Information, Speaker Biography,
4	Chapter Program Schedule
5	Membership Renewal, A Great Deal for New Members, Research Spotlight and Research Update
6	Certification/Exam Updates and Notice of Fraudulent Website
7	Have you reviewed K-NET® recently?
8	Conferences & Financial Update
9	Chapter Board Roster

December 2006

# Newsletter

---



Dear Members,

It's hard to believe that it's almost the end of the year, and we're already half way through our program year. The new chapter year has started off wonderfully with great meetings and attendance.

Thank you for making our November breakfast meeting a big success. Clint Hatton did a wonderful job presenting "Following the Bread Crumbs -- Penetration Testing and the Role of Vulnerability Assessments Scanners". The meeting was interactive, with a lot of dialog, and Clint fielded a number of questions and comments from the audience. Please refer to our website for a copy of the meeting's presentation materials. Our breakfast meetings have definitely been a hit and we will continue with this meeting format going forward.

For your convenience, we are presenting our 2nd annual series of **free Webinars**, worth **1 CPE**, each. Once again, SPI Dynamics has offered to present the Webinars, based on topics you've suggested through our annual survey. Please refer to page two of this Newsletter for more details on December's Webinar topic: "Hacking AJAX-based Web Applications". Last year's Webinars were a big success and I hope you'll join us for our free Webinars in December and January, too!

For those of you taking the CISA and CISM exam this month (We have 8 chapter members taking the exams), we wish you the best of luck and look forward to welcoming you to the ranks of CISAs and CISM's around the world!

Happy Holidays,

John Juarez, CISA  
President

December 2006

# Newsletter



## December Webinar Synopsis

### “Hacking AJAX-based Web Applications”

Clint Hatton will demonstrate how AJAX is vulnerable to threats typically associated with Web applications with examples of hacking techniques used to compromise an application using AJAX. In addition, the presentation will explore how the technology underlying Ajax opens up a number of other interesting vulnerabilities that all organizations looking to deploy Ajax should be aware of.

AJAX (Asynchronous JavaScript and XML), which is a method of building interactive applications for the Web that process user requests immediately. AJAX is an aggressively evolving software development technology used by industry leaders such as Google and Microsoft. However, this new technology presents many security concerns because AJAX-based applications are susceptible to the same types of common vulnerabilities overwhelmingly found in Web applications; they are just easier to attack and much more difficult to test and defend.

### Speaker Biography

Clint Hatton is a senior security engineer for SPI Dynamics ([www.spidynamics.com](http://www.spidynamics.com)), the expert in Web application security assessment and testing. He has over 20 years experience in the information technology industry. Clint recently founded an organization that refurbishes used and donated corporate computer equipment, in his spare time he provides equipment, training, and support to the elderly and needy.

### CPE & Registration Information

**Date/Time & Location:** Anytime/anywhere/Internet during December. To receive a link to the Webinar, please register by contacting Dan Moyer at [secretary@wmisaca.org](mailto:secretary@wmisaca.org) or 517-323-7000 x3102, or after November 23, 2006 register on-line at [www.wmisaca.org](http://www.wmisaca.org).

**Cost:** Free.

**CPE credit:** 1 Hr. After registering, Dan will provide you with a CPE certificate.

December 2006



# Newsletter

---

**Western Michigan  
Information Systems Audit & Control Association  
2006 – 2007 Program Year**

**December 2006**

**Topic: Webinar - “Hacking AJAX-based Web Applications”**

Time: Anytime/Anywhere during December

Presenter: Clint Hatton, SPI Dynamics

CPE: 1 Hr

**January 2007**

**Topic: Webinar - “Advanced Web Application Attacks: Methodologies and Demonstrations of Web Application Hacks”**

Presenter: Clint Hatton, SPI Dynamics

CPE: 1 Hr

**February 2007**

**Topic: Student Night – Joint ISACA/IIA Meeting**

**March 2007**

**Topic: 1 Day Training Seminar**

Location: Grand Rapids, Michigan

**April 2007**

**Topic: 1 Day Training Seminar**

Location: Lansing, Michigan

**May 2007**

**Topic: 1<sup>st</sup> Annual Awards Meeting**

Location: Lansing & Grand Rapids, Michigan

# Newsletter

---

## Membership Renewal

In the next few weeks, it will once again be renewal season at ISACA. All members will have the opportunity to easily renew their membership online by logging on to the ISACA web site. You are encouraged to renew online to help keep ISACA membership as cost-effective as possible.

## Great Deal for New Members

If you're not already a member, you should know about ISACA's new incentive this year. If you are joining as a new member between now and December 31, 2006, you get more for your money! You pay the annual International association dues, the new member processing fee and chapter dues, but your membership doesn't expire until **December 31, 2007**. In addition, register online at [www.isaca.org](http://www.isaca.org) and the new member processing fee is reduced from \$30 to \$10.

## Research Spotlight

### ***COBIT<sup>®</sup> Mapping: Mapping of PRINCE2 With COBIT<sup>®</sup> 4.0***

Projects in Controlled Environments (PRINCE) is a structured method for project management. The PRINCE method was first established in 1989 by the UK Central Computer and Telecommunications Agency (CCTA), now the UK Office of Government Commerce (OGC). The detailed mapping consists of the information requirements of PRINCE2 that were mapped to COBIT control objectives. The structure follows the domains, processes and control objectives of COBIT. It will post as a complimentary download for ISACA members during December at [www.isaca.org/downloads](http://www.isaca.org/downloads).

## Research Update

### ***COBIT<sup>®</sup> Mapping: Mapping of ITIL With COBIT<sup>®</sup> 4.0***

The Information Technology Infrastructure Library (ITIL), released by the OGC, consists of 10 processes—more commonly understood as service support (operational) and service delivery (tactical) processes—that comprise one function, effective IT service management. This mapping document contains a detailed mapping of ITIL with COBIT 4.0. It will post as a complimentary download for ISACA members during December at [www.isaca.org/downloads](http://www.isaca.org/downloads).

### ***COBIT<sup>®</sup> Mapping: Mapping of TOGAF With COBIT<sup>®</sup> 4.0***

The Open Group Architecture Framework (TOGAF) is a detailed method and set of supporting tools for developing enterprise architecture. It was developed by members of The Open Group, working within the Architecture Forum and has been in existence since 1995. This mapping document contains a detailed mapping of TOGAF 8.1 with COBIT 4.0. The structure follows the domains, processes and control objectives of COBIT. It will be posted as a complimentary download for ISACA members in the first quarter of 2007 at [www.isaca.org/downloads](http://www.isaca.org/downloads).

### ***COBIT<sup>®</sup> Mapping: Mapping of ISO/IEC 17799:2005 With COBIT<sup>®</sup> 4.0***

ISO/IEC 17799:2005 *The Code of Practice for Information Security Management* is an international standard based on BS 7799-1/ISO/IEC 17799:2000. It is presented as best practice for implementing information security management. This mapping document contains a detailed mapping of ISO/IEC 17799:2005 with COBIT 4.0. It will be posted as a complimentary download for ISACA members in the first quarter of 2007 at [www.isaca.org/downloads](http://www.isaca.org/downloads).

December 2006

# Newsletter



## **Certification/Exam Updates**

The CISM exam in December 2006 will be the last exam using the current CISM job practice areas and candidates should use the 2006 CISM study materials (not those that will soon be available for the 2007 exam).

Registration for the December exam administrations closed with more than **13,300** Certified Information Systems Auditor™ (CISA®) and **2,000** Certified Information Security Manager® (CISM®) exam registrants. Approximately eight weeks after the test date, the official exam results will be mailed to candidates. Additionally, with the candidate's consent to item 25 on the registration form and payment in full, an e-mail containing the candidate's pass/fail status and score will be sent to the address listed in the candidate's profile at the time of the initial release of the results. To ensure the confidentiality of scores, exam results will not be reported by telephone or fax. Candidates should add [certification@isaca.org](mailto:certification@isaca.org) to their address book, white list or safe-senders list.

Registration for the June 2007 CISA and CISM exams began the second week of November. Candidates may view or print a copy of the CISA or CISM Bulletin of Information for the June 2007 exams at [www.isaca.org/cisaboi](http://www.isaca.org/cisaboi) and [www.isaca.org/cismboi](http://www.isaca.org/cismboi).

## ***CISA and CISM Scoring Change***

ISACA's CISA and CISM certification boards recently approved changing the way exams are scored. To alleviate confusion with the previous scoring method and provide greater clarity, ISACA will use a 200-800 point scale with a passing point of 450, beginning with the June 2007 exam. Using a 200-800 scale will increase the range of scores and also eliminate the perception that the score is a percentage. This scoring method is used by several testing organizations, including the well-respected SAT and GRE exams.

## ***Certification Renewals***

Please submit your annual membership fees and any associated certification fees and continuing professional education (CPE) hours by 15 January 2007. For reference regarding qualifying activities and the calculation formula, the CPE policy is available at [www.isaca.org/cisacpepolicy](http://www.isaca.org/cisacpepolicy) or [www.isaca.org/cismcpepolicy](http://www.isaca.org/cismcpepolicy). If further explanation is needed, please direct your questions to the certification department.

## **Fraudulent Chinese Web Site**

In May, a notice was posted regarding a web site ([www.cisaca.org](http://www.cisaca.org)) originating in China fraudulently claiming to be authorized by ISACA to register candidates for the CISA exam and to collect exam fees through its site. ISACA has also been informed that [www.cisaca.com](http://www.cisaca.com) is a related site with similar claims. Please be advised that neither of these web sites nor their owners are affiliated in any way with or endorsed by ISACA—nor have these web sites or their owners been authorized as registrars for the CISA exam or as distributors of any CISA study materials.

If you are aware of any similar situations occurring in our geographic area, please contact the certification department at International Headquarters immediately. If you have been adversely impacted by these web sites please contact the certification department at [certification@isaca.org](mailto:certification@isaca.org). Online registration for the CISA and CISM exams can be completed only through the ISACA web site ([www.isaca.org/examreg](http://www.isaca.org/examreg)) or via fax/mail to ISACA International Headquarters. ■

December 2006

# Newsletter

---



## **Have you reviewed K-NET® recently?**

K-NET® is an Internet-based database of knowledge specifically developed to provide ISACA® members with direct access to educational opportunities, books and CDs, articles and papers, and web resources relevant to information systems governance, control, security and assurance. For K-NET, pertinent knowledge has been sought, identified and peer-reviewed by volunteers who are practicing IT professionals. The references have then been organized into logical categories of interest to ISACA members and other constituents.

K-NET includes:

- \* Full access for ISACA members
- \* 13 subject areas
- \* More than 180 topic areas
- \* More than 6,000 knowledge references
- \* Weekly updates
- \* Search engines
- \* Personalization features

K-NET's personalized service enables members to remain current on the topic areas most important to them. ISACA members may request and receive weekly e-mails about new references that have been added within their specified areas of interest. To activate this personalized service and register to receive updates on topics of interest, visit [www.isaca.org/KNET](http://www.isaca.org/KNET) and click on TRACK UPDATES on any interior page.



# Newsletter

**Conferences**

New 2006-2007 ISACA conference and educational event dates have been released. For the latest information and a complete listing, please visit [www.isaca.org/conferences](http://www.isaca.org/conferences).

**2006-2007 Conference/Training Week Calendar**

	ISACA Training Week	COBIT User Convention	Information Security Conference	ISACA Training Week	Euro CACS <sup>sm</sup>	North America CACS <sup>sm</sup>	ISACA Training Week	International Conference	Oceania CACS <sup>sm</sup>
<b>Dates</b>	4-8 December 2006	18-19 January 2007	5-7 February 2007	26 February-2 March 2007	18-21 March 2007	22-26 April 2007	7-11 May 2007	22-25 July 2007	9-12 September 2007
<b>Location</b>	Orlando, Florida, USA	Pasadena, California, USA	Panama City, Panama	Washington DC, USA	Vienna, Austria	Grapevine, Texas, USA	Denver, Colorado, USA	Singapore	Auckland, New Zealand
<b>CPE Hours</b>	38	13	21	38	40	44	38	TBA	TBA

**Financial Statement**

**ISACA West Michigan Statement of Financial Position  
as of 7/31/2006**

Account	7/1/2006	7/31/2006
<b>ASSETS</b>		
Cash	\$ 14,722.22	\$ 14,662.13
NC CD - 6 month (7365231096)	5,124.34	5,138.89
	<u>\$ 19,846.56</u>	<u>\$ 19,801.02</u>
<b>NET ASSETS</b>		
Temporarily Restricted	5,124.34	5,138.89
Unrestricted	14,722.22	14,662.13
<b>TOTAL NET ASSETS</b>	<u>\$ 19,846.56</u>	<u>\$ 19,801.02</u>

**ISACA West Michigan Statement of Cash Flow  
07/01/2006 through 7/31/2006**

Net Assets, Beginning (7/01/2006)	\$ 19,846.56
Change in Net Assets	\$ (45.54)
Net Assets, Ending (7/31/2006)	<u>\$ 19,801.02</u>

December 2006

# Newsletter

---



## Officers

### President

John Juarez, CISA  
Michigan Department of Management and Budget  
(517) 241-2713  
[juarezj@michigan.gov](mailto:juarezj@michigan.gov)

### Vice President

Joseph Campbell  
Express-1, Inc  
(269) 695-2700  
[Joe.Campbell@express-1.com](mailto:Joe.Campbell@express-1.com)

### Secretary

Dan Moyer  
Michigan Farm Bureau  
517-323-7000 ext. 3102  
[dmoyer@michfb.com](mailto:dmoyer@michfb.com)

### Treasurer

Lori Mullins, CISA  
Michigan Office of the Auditor General  
(517) 334-8050  
[MullinsL@michigan.gov](mailto:MullinsL@michigan.gov)

## Directors

### Director At-Large

Sandy Streb, CPA, CISA  
Michigan Department of Management and Budget  
(517) 322-1603  
[StrebS@michigan.gov](mailto:StrebS@michigan.gov)

### CISA/CISM

#### Coordinator

Ted Keniston  
517-230-5961  
[certification@wmisaca.org](mailto:certification@wmisaca.org)

### Webmaster

Don McNally  
National City Corporation  
(269) 973-2293  
[Donald.McNally@nationalcity.com](mailto:Donald.McNally@nationalcity.com)

### Past President

Richard Rosenthal  
State Employees Credit Union  
(517) 267-7427  
[RRosenthal@secu.org](mailto:RRosenthal@secu.org)

### Website

<http://www.wmisaca.org/>