

**OFFICERS
AND
DIRECTORS
2003-2004**

PRESIDENT

John W. McCormick, CISA, CIA
(248) 471-3075

VICE PRESIDENT

Karine F. Wegrzynowicz, CISA
Ford Motor Company
(313) 337-5796

TREASURER

Brenda L. Karl, CISA
Jefferson Wells International
(248) 350-3006

SECRETARY

Patricia A. Earl-Cole, CISA, CIA
Blue Cross Blue Shield of MI
(313) 225-7598

DIRECTORS

Arthur Abruzzo, CISA, CDP, CSP
Amerisure Companies
(248) 426-7944

Salman Aziz
Delphi Automotive
(248) 813-8034

Edward R. Barszcz, CIA, CFE
Blue Cross Blue Shield of MI
(313) 225-9076

Gerald Baumgart, CISA
Retired

Michael A. Forrest, CISA
Jefferson Wells International
(248) 350-3006

Paul L. Haley, CISA
DTE Energy
(313) 235-9244

John H. Hoppesch, CISA
The Auto Group
(313) 336-8725

Michael D. Mullens, CISA, CIA
General Motors Corporation
(588) 382-1543

Robert J. Otten, CISA, CIA
Kmart Corporation
(248) 463-2428

Brandy A. Pfeiffer, CISA, CPA
Federal-Mogul Corporation
(248) 354-2602

John L. Quaine II, CISA, CPA, CIA
Blue Cross Blue Shield of MI
(313) 225-7663

Carrie E. Schrader, CISA, CBM
Deloitte & Touche LLP
(313) 396-2754

Michael S. Stolarczyk, CISA
Jefferson Wells International
(248) 226-1319

David F. Thompson, CISA, CFE
Blue Cross Blue Shield of MI
(313) 225-6384

Douglas S. Wahr, CISA, CISSP
The Auto Club Group
(313) 436-7488

Robert V. Yanik, CISA
City of Detroit
(313) 224-3101



Information Systems
Audit and Control
Association

DATA BYTE

NEWSLETTER OF THE DETROIT AREA CHAPTER

VOLUME 18, #1

REGION 2, CHAPTER 8

SEPTEMBER, 2003

Monthly Meeting Wednesday, September 17, 2003

Pre-Dinner Topic: "CISCO Equipment – Audit Issues & Best Practices"
Thomas Wallace

After-Dinner Topic: "Effective Interviewing"
Richard Percy and Mark W. Warner, CFE

Date: Wednesday, September 17, 2003

Time: 4:30-5:00 Registration/Networking
5:00-6:00 Before-Dinner Presentation
6:00-7:00 Dinner
7:00-8:00 After-Dinner Presentation

**PLEASE NOTE NEW MEETING LOCATION AND PRICING BELOW
MAP AND DIRECTIONS ON PAGE 5**

Location: Tapestry
24580 Evergreen
Southfield, Michigan 48075
(248) 722-1547

Cost: \$25.00 Members
\$35.00 Non-Members
\$10.00 Students and Retirees

Reservations will be taken by Suzanne McCormick. Please make reservations by NOON on Friday, September 12, 2003. You can make your reservation online at isaca-det.org or e-mail your reservation to Suzanne McCormick at jsmccor65@aol.com. If you do not have access to the Internet, call Suzanne at (248) 471-3075. Please include your name, certification, company, telephone number, and whether you are a Member, Non-member, Student or Retiree. All e-mail reservations will receive a personal confirmation that the reservation was received. Walk-ins are welcome.

Visit our web site at: isaca-det.org

Letter from the President

Dear Members,

Welcome to the start of our 2003-2004 chapter year. The 2003 summer months have been very busy and productive! Our Program Committee has put together an exciting agenda for the nine meetings this year. You may refer to "A Year at a Glance" section elsewhere in this newsletter to review the subject matter of each meeting. It is our goal to provide you with advance notice of upcoming meetings so that you may plan your training needs accordingly. As seminars are developed, we also will be informing you of their content as soon as they are formalized.

Please note the references throughout this newsletter to our new meeting location at the Tapestry at Ten Mile Road and the Lodge in Southfield. We have had two chapter board meetings there and the service, food, accommodations and location are great!

One of our more important goals is to communicate with our membership electronically. To that end, we are updating, with your assistance, our directory of email addresses for members and attendees. In June, we were invited to be the guests of the Detroit Area chapter of the Information Systems Security Association (ISSA) and we were able to quickly get the word out to our members for whom we had up-to-date email addresses. The affair was such a success that we are contemplating doing it again next year. Starting with this newsletter, we will be sending a hard copy to you and an electronic PDF copy if we have your email address. Our goal is to eventually reduce our dependence on hard copy to only those individuals who cannot or will not accept only an electronic copy. Your cooperation in the next few months in communicating to our chapter administrator (Suzanne McCormick jmccor65@aol.com) your email address will expedite the successful conclusion of this project.

The chapter leadership has decided to try a number of new things this year, i.e. relocating to a new meeting facility, communicating electronically where possible, making a strong drive to invite new industry to our meetings, outsourcing many of our administrative responsibilities, growing our chapter attendance by at least 50%, promoting IT internships, and always improving our selection of training speakers both at

chapter meetings and seminars. Our goals are to provide a professional service to and growth of our membership.

At the International ISACA

The benefit of belonging to an international organization is that we can leverage off of their awareness of industry trends, training possibilities, availability of tools, etc.

One such jewel at www.isaca.org is a site called KNET. Much of the content of KNET is available to anyone on the web. Some key areas currently out there are: *IS Audit Control Security (Tools, Environments, general)*, *IS Security*, *IS Control*, *IT Governance*, *eBusiness*, *Telecommunications*, *Project Management*, *Education*, *Publications*, *Standards*, and *Professional Development*. Contained within these categories are tools, program guides, research, as well as other topics. Much of the better materials, however, do require you to provide an ISACA member ID and password and if you have forgotten them, the site assists you in finding out what they are.

To support your training needs, the International publishes a calendar of upcoming training. In September, there is a Network Security Conference, the Oceania CACS conference and an IS Audit and Control Training week. In October, look for the Latin American CACS conference, and two different IS Audit & Control Training weeks. The International also reminds you that your opportunity to grandfather the CISM ends December 31, 2003. You may visit www.isaca.org/cism.htm for more information.

Back at home,

Our September meeting promises to be both informative and fun. We are presenting an excellent pre-dinner technical topic, CISCO products, followed by an after dinner presentation on interview techniques by two gentlemen who have seen the best and worse in people, both in police work and IS Security. Additionally, our facilities chairperson has ordered a meal that will have you coming back for more. Great speakers, food, and networking! We hope we see you there.

John W. McCormick, CISA, CIA
President
Detroit Chapter ISACA

PRE-DINNER INFORMATION**“CISCO Equipment – Audit Issues & Best Practices”**

Thomas Wallace

Need information about product functionality, switches, segmenting, and managing router configuration files? CISCO Systems has suggestions on good practices for initial design, planning, installation and testing. Tom has websites containing standards to reference as explained in Cisco whitepapers or available from Cisco Systems. A discussion will be given on how CISCO tools could have mitigated the August Internet worms.

Thomas Wallace is a Security Specialist with CISCO Systems Inc. with responsibility for the upper mid-west territory.

New Board Member

Robert J. Otten, CIA, CISA

Rob is a senior auditor for Kmart Corporation where he is engaged in the COSO/COBIT implementation project for Sarbanes-Oxley Compliance. He has previously served the Membership by working on various other committees. Please join us in welcoming Rob to the Board.

2003-2004 Committees**CISA**Dave Thompson – Chair – dthompsn@bcbsm.com**FACILITIES**Ed Barszcz – Co-Chair – ebarszcz@bcbsm.comJohn Hoppesch – Co Chair - jhoppesch@yahoo.com**INTERNET**Brandy Pfeiffer – Chair – brandy_pfeiffer@fmo.com**SEMINARS**Karine Wegrzynowicz – Co-Chair – kwegrzy@ford.com

Mike Stolarczyk – Co Chair –

mike_stolarczyk@jeffersonwells.com**MEMBERSHIP/ACADEMIC RELATIONS**Patti Earl-Cole – Co-Chair – pcole@bcbsm.comRob Otten – Co-Chair – rotten@kmart.com**NEWSLETTER**Patti Earl-Cole - Chair – pcole@bcbsm.com**NOMINATING**Art Abruzzo – Chair – aabruzzo@amerisure.com**PROGRAMS**Paul Haley – Chair – haleyv@dteemergy.com**AFTER DINNER INFORMATION****“Effective Interviewing”**

Richard Percy and Mark W. Warner, CFE

During the presentation we will describe the difference between an interview and an interrogation. We will provide you with a fairly standard definition of both. We will cover the three main types of interviews and what they are used for and how they are differentiated. We will describe how everyone has and continually does utilize interviewing techniques in their daily lives. We will provide the group with useful tips to enhance their information gathering skills both on the job and in their personal life.

Richard Percy began his career as an auditor with the American National Holding Company where he was responsible for Branch and Affiliate Bank Audits.

In 1974 he joined the Michigan Department of State Police as a Trooper. While with the Michigan Department of State Police he served as a Detective Sergeant and as a Detective Lieutenant.

Following his retirement 1999 Richard worked for the Michigan Gaming Control Board where he was responsible for conducting licensure suitability audits on multinational gaming companies.

Richard joined Jefferson Wells International as a Fraud Investigator in 2001.

Richard is a graduate of Western Michigan University and has been certified in personal interview techniques and Scientific Content Analysis (SCAN).

Mark Warner has over 30 years experience in law enforcement, criminal investigations, private security, and accounting. During that time he has conducted numerous investigations to accomplish varied goals from criminal prosecution to internal corporate investigations.

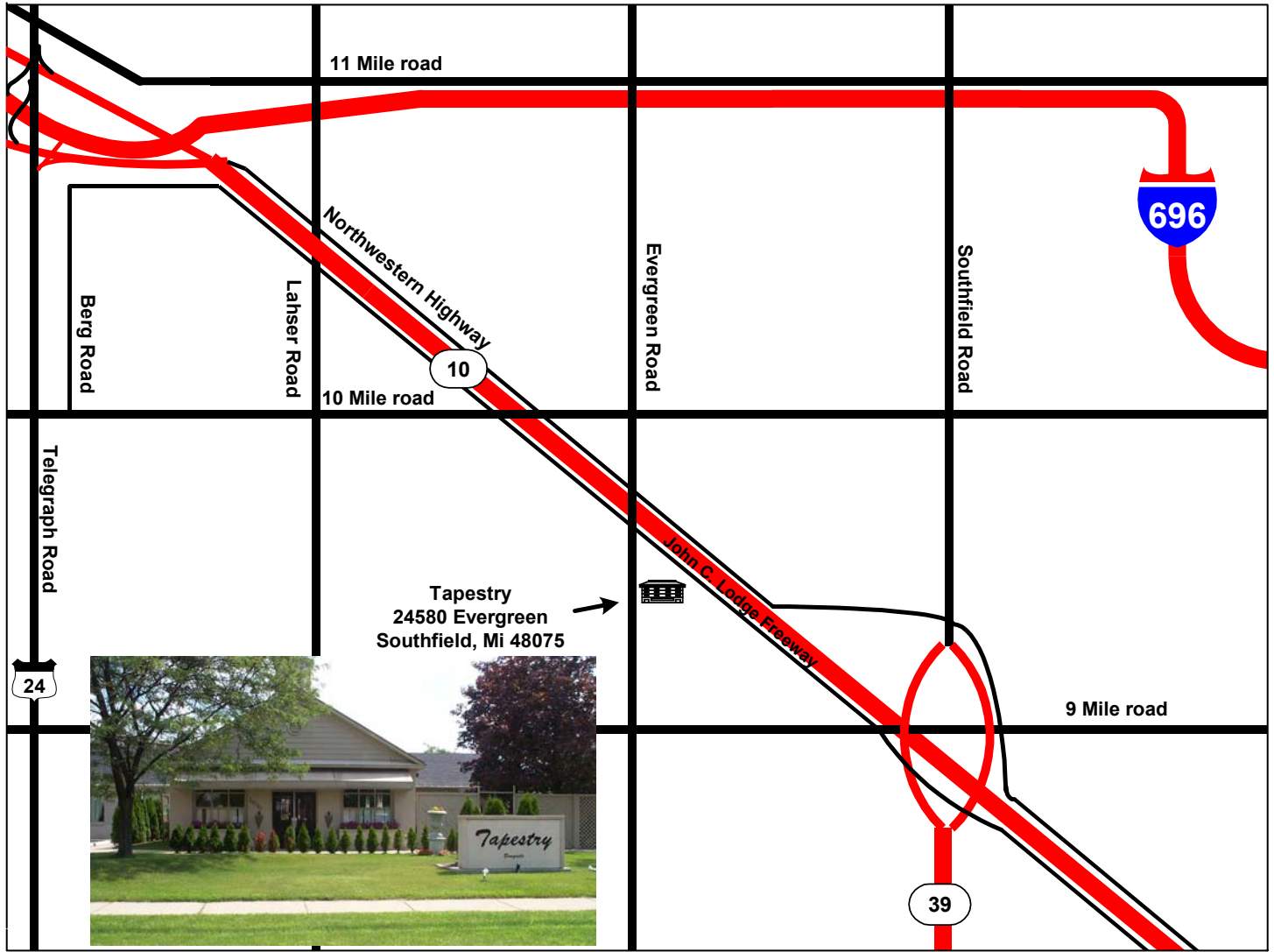
Upon completing his military service and returning to Michigan he entered the Michigan Department of State Police in February of 1974. Over a 14-year period Mark worked in a wide range of assignments from uniformed patrol to undercover narcotics investigations.

Mark obtained his BS from the University of Michigan Dearborn in 1988 leaving the Department for public accounting. Between 1988 and 1993 he worked for an international accounting firm and two small local firms. In 1993 Mark returned to law enforcement. Shortly thereafter Mark entered the private investigation and security field. He has held positions from senior investigator to director of operations.

Mark also is trained in the Scientific Content Analysis (SCAN) method of statement interpretation.

YEAR AT A GLANCE

September 12, 2003	Reservations due by noon for the September 17 ISACA dinner meeting
September 16, 2003	Deadline for the October issue of the Databyte
September 17, 2003	Chapter Meeting “CISCO Equipment – Audit Issues & Best Practices” – Thomas Wallace Interview Techniques” – Richard Percy and Mark W. Warner, CFE
October 10, 2003	Reservations due by noon for the October 15 ISACA dinner meeting
October 14, 2003	Deadline for the November issue of the Databyte
October 15, 2003	Chapter Meeting “Virtual Private Network (VPN) Audit Program” - Roger Younglove “Enterprise Resource Planning (ERP) & Systems Development Life Cycle (SDLC) – New ISACA Practices”
November 11, 2003	Deadline for the December issue of the Databyte
November 14, 2003	Reservations due by noon for the November 19 ISACA dinner meeting
November 19, 2003	Chapter Meeting “Audit of Patches to Servers/PCs” “Sarbanes Oxley”
December 5, 2003	Reservations due by noon for the December 9 ISACA/IIA dinner meeting
December 9, 2003	Chapter Meeting <i>Joint meeting with the IIA</i> “HIPAA” – Doug Volinski
December 9, 2003	Deadline for the January issue of the Databyte
January 9, 2004	Reservations due by noon for the January 15 ISACA/CFE dinner meeting
January 13, 2004	Deadline for the February issue of the Databyte
January 14, 2004	Chapter Meeting <i>Joint meeting with the CFE</i> “Forensic Auditing” – Roy Parry
February, 2004	Early Registration Deadline for June 2004 CISA and CISM Exam – Actual date to be announced at a later time
February 12, 2004	Deadline for the March issue of the Databyte
February 13, 2004	Reservations due by noon for the February 18 ISACA dinner meeting
February 18, 2004	Chapter Meeting “Thesis: Security Concepts” – Rob Otten “Audits, Audit Work Papers, Discovery”
March 11, 2004	Deadline for the April issue of the Databyte
March 12, 2004	Reservations due by noon for the March 17 ISACA dinner meeting
March 17, 2004	Chapter Meeting <i>Student Night</i> “Panel Discussion on Skill Sets” “Disaster Communication Capacity/Planning” – Thomas Raupp
March 22 – March 24, 2004	ISACA/IIA Spring Seminar
April, 2004	Final Registration for June 2004 CISA and CISM Exam – Actual date to be announced at a later time
April 16, 2004	Reservations due by noon for the April 21 ISACA dinner meeting
April 20, 2004	Deadline for the May issue of the Databyte
April 21, 2004	Chapter Meeting “Lightweight Directory Access Protocol (LDAP) Audit Program” “Electric Choice and Energy Audits” – Joe McCormick
May 14, 2004	Reservations due by noon for the May 19 ISACA dinner meeting
May 19, 2004	Chapter Meeting “MS Access – How to Use in an Audit” – Mike Stolarczyk and Paul Haley Above topic and speakers for both pre-dinner and after-dinner
June, 2004	CISA and CISM exam – Actual date to be announced at a later time



TAPESTRY

24580 Evergreen
 Southfield, Michigan 48075
 (248) 722-1547

Tapestry is located near major freeways. It is ¼ mile from Highway 10 (the Lodge) and just 1 mile south of I-696 on Evergreen. Tapestry is south of the Speedway Gas station that is located on the SE corner of the Lodge and Evergreen. Tapestry is on the East side of Evergreen Road and is a single story dark beige building. (It was previously a Bill Knapp’s restaurant)

From the Troy Area: Take I-75 South to 696 West. Take 696 West to Exit #11 Evergreen Road. Turn left onto Evergreen Road. Tapestry is just over a mile (1.1) on the left hand side (East side) of Evergreen.

From Detroit: Take The John C. Lodge MI-10 North out of Detroit. Take the Lodge North until the Ten (10) Mile Evergreen Road Exit. Turn left onto Evergreen Road. Evergreen is the first major intersection off of the Lodge. Tapestry Restaurant is only a tenth of a mile on Evergreen on the left hand side. (East side).

From Farmington/Novi Area: Take 696 East (Walter P. Reuther) to the John C. Lodge MI 10 South. Follow the John C. Lodge MI 10 for 2 ½ miles to the Evergreen Ten (10) Mile Road Exit. Follow the service drive to Evergreen Road (past 10 Mile Road) and turn Right. Tapestry is less than a tenth of a mile on Evergreen on the left hand side (East side).

From Dearborn/South/Southwest Area: Go to Telegraph Road. Take Telegraph North to Nine (9) Mile Road. Turn right onto Nine Mile to go East. Take Nine Mile for approximately 2 Miles to Evergreen and turn left. Take Evergreen North less than a mile and Tapestry is on your right (East) before 10 Mile Road.

Risk Assessment/Business Impact Analysis

By JOHN M. DUKE
BCBSM

The Professional Practices for Business Continuity Planners describes the Risk Assessment/Business Impact Analysis (RA/BIA) as the single, most important factor driving business recovery planning. The RA/BIA identifies the requirements and priorities that provide the basis for the business recovery plan.

This product is the result of a two pronged approach. The Risk Analysis is a process designed to identify, document and rank the risks to an organization. The Business Impact Analysis identifies critical business functions of the organization and the resources necessary to support those functions. It also quantifies the impact a business disruption would have.

The steps in the Risk Analysis process include:

- Identification of potential risks to the organization
- Identification of outside expertise that may be required
- Identification of vulnerabilities/threats/exposures
- Identification of risk reduction/mitigation alternatives
- Identification of credible information sources
- Determination of acceptable risk levels

It is important to note that in this type of risk assessment, the risks are generally specifically quantified. Rather than working with a generic matrix of low, medium and high risk, a measurable probability factor is assigned to each threat. As an example, rather than identifying Tornado as a high probability, a specific quantitative probability factor of .02 might be assigned to this threat, based upon available geographical and meteorological statistical data.

The Business Impact Analysis process includes:

- Identification of the organization's critical business functions
- Identification of process and resource relationships
- Identification of interdependencies
- Definition of recovery objectives and timeframes
- Identification of resource requirements
- Identification of information requirements

The Business Impact Analysis is also quantified. This figure is generally expressed in the cost per day of the loss or interruption of a critical business functionality such as sales, service, accounting, etc. As an example, the loss of the ability to ship product might be quantified as costing an organization \$750,000 per day. The cost typically could increase exponentially with the length of the outage.

The information that is quantified in a RA/BIA enables an organization to identify those threats that are most likely to occur and the level of risk that they pose. This ranking provides the platform to prioritize the risks. Steps may then be taken to remove the risk, to mitigate it, or to develop contingency plans to deal with the event if it should occur. It also helps to determine those risks that, because of their relatively low probability of occurrence, can be accepted without potentially costly mitigation planning.

The impact the risk could have on an organization is also described in terms of cost. This provides senior management with cost-benefit information upon which to base the decisions regarding the direction of their business recovery and disaster recovery planning. This cost-benefit information, along with information regarding interdependencies, is also used to make decisions regarding Recovery Time Objectives (RTO) and Recovery Point Objective (RPO).

RTOs define how soon systems must be recovered after interruption. Some organizations might be able to accommodate to a RTO of 96 hours while others might need a much faster recovery. RPOs define the point in time (relative to data accuracy) to which they might recover. Some organizations might be able to recover to data that is 24 hours or more old, since they have the ability to recreate the lost data. Other organizations might require complete recovery to the point of failure. This is all dependent upon the nature of the business and the relative cost impact of an interruption of services.

Continued on Page 7

Continued from Page 6

The complexity of the business and disaster recovery plans as well as the budget and resources necessary to support the planning initiative should be directly related to the information provided through the RA/BIA. When performing a review of Disaster Recovery or Business Recovery plans, the RA/BIA is a recommended place to start. Certain questions should be included as a starting point for the audit program; for example:

- Has a RA/BIA been performed?
- How often is the RA/BIA refreshed or updated?
- Have the results of the RA/BIA been communicated to and supported by senior management?
- Are the elements of the business recovery and/or disaster recovery plans consistent with the results of the RA/BIA?
- Are Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO) consistent with the requirements resulting from the RA/BIA?

The actual business recovery and disaster recovery plans should directly correspond to the requirements identified by the RA/BIA. Once an auditor has verified the validity of the business recovery and disaster recovery plans with regard to the RA/BIA, only then should they proceed to more detailed examination of the plans themselves.

"The most effective disaster recovery plan is an updated copy of one's resume, stored in a secure off-site location." Old adage.

John Duke is currently a Principal IS Auditor for BCBSM. He has over 40 years experience in all phases of Information Systems, including audit and controls as well as disaster recovery and business recovery. He recently qualified for certification as a Certified Business Continuity Professional (CBCP) and serves as a facilitator for the Disaster Recovery and Business Continuity portion of the CISA Review Course. If you or your organization have need of more information you may contact him at jduke@bcbsm.com

Recent ISACA Certifications

CISA Certification

Michael Norman Juchno

CISM Certification

Aaron Ely Earle
Thomas Spencer Fielitz
Geraldine Hanspard
Dr. Linda M. Kinczkowski
Justin Aaron Peltier
Thomas Richard Peltier
Donald T. Wang

Wanted

Organizations Promoting Academic Excellence

The Detroit Chapter is encouraging all organizations committed to learning to express their commitments by hosting an Intern through the ISACA Detroit Internship program. The benefits of Internships to students who demonstrate academic excellence is unlimited. The ability to obtain direct experience prior to graduation enhances student's success upon entry into the profession. An internship can also be a rewarding experience for the organization. Students who are eligible to participate in ISACA Detroit's program are from schools recognized for their IT Audit curriculums and are prepared to execute most staff level assignments. Therefore the program increases the chances of selecting a qualified candidate. Also, since Internships are scheduled for a fix length of time they are cost effective solutions for short term assignments and special projects.

If you are interested in details of the ISACA Detroit Internship program, please contact Robert Otten at rotten@kmart.com

For a list of ISACA endorsed curriculums, please visit <http://www.isaca.org/univ1.htm>

Monthly Highlights

September 12, 2003
September 16, 2003
September 17, 2003

Reservations due by **NOON** for the September 17 ISACA dinner meeting
Deadline for information for the October issue of the Databyte
September ISACA dinner meeting
“CISCO Equipment - Audit Issues & Best Practices”
“Effective Interviewing”

Menu – September 17, 2003

THE SEPTEMBER MEETING WILL A DINNER BUFFET

FIELD GREENS with
Mandarin Oranges and Raspberry Vinaigrette
BEEF TENDERLOIN – Carved to Order
BREAST OF CHICKEN PICATTA
with Artichokes, Capers and Lemon
SUPERIOR WHITEFISH FILET
with Capers and Lemon Beurre Blanc
GREEN BEANS ALMONDINE
GARLIC-MASHED YUKON GOLD POTATOES
ASSORTED MINI PASTRIES
COFFEE, TEA, POP AVAILABLE WITH DINNER



OPEN BAR

BEER AND WINE ONLY
NO OTHER LIQUOR AVAILABLE

VEGETARIAN PLATE AVAILABLE
(VEGETARIAN PLATE AVAILABLE BY PRE-REGISTRATION ONLY)

The Chapter must provide the number of reservations by 4:00 p.m. on the Friday before the meeting. To ensure that we can accommodate those who wish to attend and the facility can provide the best service possible, please make your reservations early. If you have made a reservation and cannot attend, please call Suzanne McCormick at (248) 471-3075. Your cooperation is greatly appreciated.

New ISACA Members

Ramit Arora
William Patrick Beaver
Thomas Spencer Fielitz
Eric V. Findley
Kelly Ann Lange
Justin Aaron Peltier
Charles E. Mason
Thomas Richard Peltier
Keith Sherman
Hadi A. Q. Siddiqui
Joanne Melissa Tsamaidis
Peter Wardrope
John Rob Wigley

DATABYTE



Information Systems
Audit and Control
Association

DETROIT AREA CHAPTER
SUZANNE McCORMICK, EDITOR
30032 FINK AVENUE
FARMINGTON HILLS, MI 48336
(248) 471-3075
Jsmccor65@aol.com