

It is our pleasure to invite you to the March chapter luncheon at Confluence Park, Columbus, Ohio. At Central Ohio ISACA, we are blessed to have within our midst outstanding professionals in the areas of IT Governance, Security, and Assurance. So, once again, we present to you one of our local talents, Mr. Michael Parkes from Crowe Horwarth LLP who will be presenting on: **GOVERNANCE, RISK MANAGEMENT AND COMPLIANCE (GRC)**.

We hope that you will find this presentation to be both insightful and of interest to you. This will also be a wonderful opportunity to network within our membership.

We appreciate your attendance and would like to encourage you to invite your colleagues and business partners. You also earn one credit hour towards your CPE.

In this newsletter you will find information on this month's presentation, a recap on our spring seminar and February meeting, and other key announcements. In addition, you will find our member spotlight and information on programs and activities sponsored by ISACA international.

CONTENTS

CHAPTER NEWS.....	1-2
PRESIDENT'S MESSAGE.....	2
INFORMATION & COMMUNICATION.....	3-4
MEMBERSHIP SPOTLIGHT.....	4
TECHINICAL EDUCATION.....	5-6

We would like to thank you for taking your time to read our chapter newsletter. Please feel free to send any comments or suggestions you may have for the newsletter or the chapter in general to us at: jothamn@gmail.com

GOVERNANCE, RISK MANAGEMENT AND COMPLIANCE (GRC)

GRC: What is it and why is it important? How does compliance differ from "good" sustainable governance? What are the elements and attributes of good governance? How can internal audit respond?

PRESENTER'S BIO:

Michael Parkes, CIA, CISA with Crowe Horwath LLP - Risk Consulting Services has 10 years of experience in internal audit and consulting, including financial, operational and information systems auditing, enterprise risk management, audit transformation and transaction services. As

a consultant at Crowe Horwath LLP, he has served a wide variety of industries including consumer products, manufacturing and distribution, telecommunications, agriculture, insurance and government. Before joining Crowe in 2004, Michael was a consultant for the Auditor of State of Ohio's office.

Michael has earned CIA and CISA designations. He is an officer in the Central Ohio Chapter of the IIA and is a member of the Central Ohio Chapter of ISACA. He has a Bachelor of Arts from Capital University in Economics.

WHERE & WHEN

Confluence Park Restaurant (679 W. Spring St., Columbus, OH 43215). The meeting starts at 11:15 a.m. with an opportunity for members to network. A presentation from Mr. Michael Parkes follows at 11:30 a.m. and lunch is served at 12:30 p.m.

The luncheon menu includes: Garden Salad, Cranberry and Wild Rice Salad, Roasted Pork Loin, Lasagna, Green Beans Almondine, Herb Whipped Potatoes, Assorted Rolls and Butter, Double Chocolate Cake, and Cherry Cobbler

We are always highlighting our local talent, i.e. our membership in the newsletter. Please feel free to use this post and submit articles, achievements, industry recognition, life, work, etc. Enjoy your reading!

RESERVATIONS

Please make your luncheon reservation via our web site at <http://www.isaca-centralohio.org/meeting.cfm> before the deadline March 09, 2009 at noon. For your convenience, the chapter currently accepts Paypal, Cash, and Checks. The cost for the luncheon is \$20 for Members, \$30 for Non-Members, and \$5 for Students. Please note that ISSA and IIA will be granted membership price.

Editorial:

Thanks - Jotham Nyamari

CHAPTER NEWS

PRESIDENT'S MESSAGE



If you have money in the stock market you may have seen a dramatic decrease in the value of the "wealth" associated with those assets. As the world economy is experiencing a severe tailspin we should not lose sight of the different measures of wealth, of which monetary is just one and certainly not the most important.

We hear it said when speaking of how wealthy someone is, that "on paper", they are worth a certain amount of money. This measure of a person's worth fluctuates with the ebb and flow of the financial markets. Other than moving a financial investment from one instrument to another, one has little actual control over its value.

There are other types of wealth with which we have a tremendous amount of control. These include the "wealth of knowledge", "wealth of influence" and "spiritual wealth". These measures of wealth, once attained, cannot be taken away from us.

I am currently reading Melvin Powers' book, "Dynamic Thinking (The Technique of Using Your Subconscious Mind)". I want

to share a quote from the book that does a wonderful job of tying together many aspects of wealth.

"...The miser Ebenezer Scrooge, in the Charles Dicken's story of Tiny Tim, never found happiness in his vast accumulation of wealth until he shared it with the family of his struggling clerk, Bob Cratchit. It was only then he found that life had a spiritual meaning. Up to then he had been leading a meaningless existence..."

I believe wealth of knowledge and wealth of influence are closely related. This is where ISACA and its tremendous wealth of resources can have a positive impact on our professional lives. The documents and literature made available by ISACA help us stay current in the technology and practice of information technology governance. More knowledge allows us to exert greater influence and increases our value and contributions to our companies.

As we progress in our adventures of life, remember the measures of our wealth and in the end, which are most important.

I look forward to seeing you at our March 12th meeting.

Brian O'Brien, CISA
President, ISACA Central Ohio Chapter

PAST EVENTS: - FEBRUARY MEETING

Mr. Kevin Saionzkowski, from the Auditor of State special audit division gave a wonderful presentation on Fraud & Investigative Auditing of Public Funds in our last month's luncheon. The meeting was very educative and informative; and answered those lingering questions about fraud in the



Kevin presenting to the chapter

public domain. For example, how does the Auditor of State know about ongoing or potential fraud, or what happens thereafter? Mr. Saionzkowski stated that the Auditor of State is made aware of potential fraud via different avenues including; a fraud hotline (1-866-FRAUD-OH), website (www.FraudOhio.com), and, but not limited to anonymous tips or letters from the public.

Members at the luncheon



What happens thereafter? Kevin explained that the Auditor of State, specifically the

PAST EVENTS: -

SECURING AND AUDITING WINDOWS SERVER AND ACTIVE DIRECTORY-

The spring seminar on Securing and Auditing Windows server and Active Directory just concluded this week. This class was very educative as it provided details and tools important in completing a successful audit of Windows server and Active Directory. Mr. Ken Cutler, an experienced instructor and practitioner in the areas of Information Technology and Security, from MIS Training Institute led this three day seminar.

We would like to thank you for your continued support in our training efforts as we strive to provide training programs that are important to you. Please let Rich Ridewood know of such needs at Richard.R.2@bwc.state.oh.us.

Special Audit Section and Special Investigations Unit, will substantiate, investigate, and quantify information received to perform a special audit. The special audit is limited in scope but thorough and uses traditional auditing procedures. In addition, Kevin provided an example of results from a special audit performed by the Auditor of State in a village in Ohio. That investigation resulted in a restitution of \$55,905.57 and a conviction of 30 days in jail. For more information on this presentation please visit our website at <http://www.isaca-centralohio.org>.



Members at the luncheon


UPCOMING EVENT:

PLEASE SAVE THE DATE (1ST WEEK OF APRIL TO 1ST WEEK OF JUNE) - CISA REVIEW CLASSES FOR JUNE EXAM

Please mark your calendars for upcoming CISA review classes starting in the first week of April to the first week of June, 2009. More information on this will be becoming soon. Also, feel free to contact Chuck Imwalle at imwalle9@gmail.com.

INFORMATION & COMMUNICATION

ISACA BENEFITS AND CALENDAR OF EVENTS

11 March, 2009	Deadline for contributions to April's COBIT® Focus
22 March, 2009	Deadline to submit nomination forms for 2009-10 ISACA International Board of Directors
23 March, 2009	Deadline for contributions to volume 4, 2009, of ISACA Journal
27 March, 2009	Deadline to apply for 2009-10 ISACA key boards and committees
	Information Security and Risk Management Conference 30-31 March 2009 (Latin America), Bogota, Colombia



Security Vulnerabilities and Safeguards (3hrs of CPE)
 31 March 2009
 8:00am PST / 11:00am EST / 4:00pm GMT

For more information on the calendar of events please visit www.isaca.org

UPCOMING EVENT: SAVE THE DATE - 3RD ANNUAL GOLF OUTING

Please mark your calendars and get you foursomes together for a great day of fun and golf.

WHEN: Friday, May 15th, 2009

WHERE: Cumberland Trail GC, Pataskala Ohio

Please contact Matthew Schondel (matthew.schondel@alliancedata.com) for more details and availability.

Sponsorship Options:

1. An overall event sponsorship (1 offered at \$1000)
2. Beverage sponsorship (1 offered at \$500)
3. Prize hole sponsorship (6 offered at \$200 each)
4. Hole sponsorship (12 offered at \$100 each)

CHAPTER LEADERSHIP

PRESIDENT

Brian O'Brien, CISA
 The Ohio State University

VICE PRESIDENT

Melissa Justice, CISA
 Ohio Office of Budget and Management

TREASURER

Mike Brady, CISA
 KPMG LLP

SECRETARY

Schlaime Hutchins, CISA, CISSP
 Cardinal Health

BOARD OF DIRECTORS

CHRIS WATSON, CISA
 SCHNEIDER DOWNS

RICH RIDWOOD, CISA, CISSP, CPA
 B.W.C. INTERNAL AUDIT DIVISION

RYAN HOUK, CISA
 AMERICAN ELECTRIC POWER

MATT SCHONDEL, CISA, CISSP
 ALLIANCE DATA

CHUCK IMWALLE, CISA, CPA, PMP

MICHAEL KIRK, CISA, CIA

JOSEPH PONNOLY, CISM, CISA, CISSP

COMMITTEE CHAIRS

ARRANGEMENTS

MELISSA JUSTICE, CISA
 OHIO AUDITOR OF STATE

MEMBERSHIP

JIM D'INNOCENZO, CISA
 THE OHIO STATE UNIVERSITY

CISA COORDINATOR

CHUCK IMWALLE, CISA, CPA, PMP

CISM COORDINATOR

JOSEPH PONNOLY, CISM, CISA, CISSP

AUDIT

GREG MASON
 STATE OF OHIO, MRDD

EDUCATION

RICH RIDWOOD, CISA, CISSP, CPA
 B.W.C. INTERNAL AUDIT DIVISION

PROGRAMS

MICHAEL KIRK, CISA

SOCIAL EVENT COORDINATOR

MATT SCHONDEL, CISA, CISSP
 ALLIANCE DATA

WEBSITE

RYAN HOUK, CISA
 AMERICAN ELECTRIC POWER

NEWSLETTER

JOTHAM NYAMARI, CISA

QUIZ TIME

Previous Question: There are known fundamental weaknesses in perimeter controls—the bad guys are frequently a step ahead of the protection and the insider threat is now recognized to be at least as serious as the threat of attack from outside the organization. Answer: True

Current: Functionality testing is designed to ensure that applications do what they are supposed to do, whereas the purpose of security testing is to check that applications do not do what they are not supposed to do. (The answer will be posted on the next newsletter)

ADAM TOOTLE, CISA
COMPLIANCE ANALYST, HONDA TRADING

EDUCATION
Bowling Green State University
B.S. MIS, Information Systems Audit & Control 2005

In my college career I started out with one major in Management Information Systems but after enjoying some of the IS audit and accounting courses; I ended up taking the advice from a fellow fraternity brother (Ryan Houk) and took on a second major in Information Systems Audit and Control. And glad I did!!

WORK:

I started my professional career in 2005 as a Compliance Analyst with Honda Trading in the IS Department at the start of their Sarbanes-Oxley remediation. I was involved in documenting control processes, IS policies and helped with the roll-out of new processes within change management, user access and system backups. I created the templates of various types of request forms for changes to financial systems and user access requests. I've now moved into the Risk Management Department to provide continuous monitoring and reporting on controls currently in place and to look for new areas to



improve. I'm highly involved in the IS Change Management process as I evaluate all requests for the appropriate approvals, testing documentation, and determine whether existing controls may be compromised. Some of my current projects are to enhance our financial application control testing and to revamp our change management process to become "paperless" with electronic approvals.

ISACA:

I was introduced to ISACA by R. Houk, went to an ISACA meeting with Cleveland chapter and joined the organization as a student member in 2004. I passed the CISA exam in 2007 and was certified in 2008, after earning enough years experience.

LIFE:

I'm originally from the small town of Circleville (home of the Pumpkin Show) so I've never been far from Columbus and all the Buckeye tail-gating that comes with it. I grew up always interested in new technology as I tinkered with my parents Compaq Presario and couldn't wait for Windows 95. Nowadays I spend my free time

trying to improve (or keep running) two computers I've built and yes I'm also a big fan of video games, mainly for the PS3. If the weather's warm, I try to get in one game of either frisbee golf or regular golf every weekend.

BOOKSTORE UPDATE

NEW CISA and CISM study aids, ISACA and ITGI research, and peer-reviewed books are offered in the ISACA Bookstore.

[Control Objectives for Information and related Technology \(COBIT\) COBIT® User Guide for Service Managers*](#) (scheduled to be available in March)

[Audit, Control and Security—Essential](#)

[The IT Regulatory and Standards Compliance Handbook: How to Survive an Information Systems Audit and Assessments](#)

[Internet and Related Security Topics](#)

[Hacking Exposed: Network Security Secrets & Solutions, 6th Edition](#)

[Audit, Control and Security Specific Environments](#)

[A Practical Guide to IBM i and i5/OS Security and Compliance](#)
[IT Governance and Business Management](#)

- Identifying and Aligning Business Goals and IT Goals: Full Research Report*
- IT Governance and Process Maturity*
- Unlocking Value: An Executive Primer on the Critical Role of IT Governance*

- The Business Value of IT: Managing Risks, Optimizing Performance and Measuring Results
- CISO Leadership: Essentials for Success
- Corporate Management, Governance, and Ethics Best Practices
- Global Perspectives in Information Security: Legal, Social, and International Issues
- Information Security Policies Made Easy, Version 11
- Service Oriented Architecture Field Guide for Executives
- CISA, CISM and CGEIT Examination References* Those preparing for the June 2009 exams should visit www.isaca.org/cisabooks, www.isaca.org/cismbooks and www.isaca.org/cgeitreferences for the new study aid editions and IT governance resources.

*ISACA/ITGI PUBLICATION

Visit ISACA Bookstore at www.isaca.org/bookstore. E-mail the Bookstore at bookstore@isaca.org or telephone +1.847.660.5650.

TECHNICAL EDUCATION

BUSINESS REFORM AND CHANGE ENABLED BY IT—AN ALTERNATIVE PERSPECTIVE IN IT GOVERNANCE

By Tony Hayes, CGEIT, FCPA, FACS, FIIA (AUS), AFCHSE, CHE

Since the beginning of the electronic age, information technology, in its various forms, has enabled business to discharge significant benefits and reforms. During these years, we have seen the automation of processes through to complex analytical innovations that have positively affected organisations at the strategic, tactical and operational service delivery levels.

These changes and reforms have touched us all regardless of our background, culture, age or location on this planet. In fact, technology-enabled benefits and achievements have been so successful in changing our lives that when access or availability is not possible, we are reminded or at least given a glimpse of life before IT. Have you experienced the pleasures of flying out of town when the airport is running on partial or no air traffic control software, finding the automated teller machines are offline, shopping when point-of-sale systems at the supermarket are not working, trying to place a call when your mobile/ cell phone network is down, or simply not being able to access the Internet?

We are totally reliant and dependent on these innovations every day of our lives. In fact, they have been so successful that we don't even think of them as technology innovations, but rather as basic commodities of life.

However, even with this background of success, innovation and change in our lives, a significant number of failures and disasters occur each day—a statistic business strives to improve through the use of IT.

IT commentators regularly remind us that more than US \$600 billion is wasted annually on ill-conceived or poorly executed IT projects. To add to this, it is often quoted that approximately 20 percent of projects fail outright, 46 percent are challenged and less than 35 percent are successful. If you are into balanced scorecards, this is not a balanced result for the industry and, more important, for organisations delivering services to their

clients/customers. My observation is that government, the not-for-profit sector and the private sector all participate in these failures. In other words, they do not occur only in the private sector.

So, with this failure rate, the successful business initiatives that have been enabled by IT must be doing something special. Or were they just lucky? Is this more about an art rather than science?

If we place a stethoscope on the failed projects to determine what went wrong, what are the symptoms? What is the diagnosis? How could failure have been prevented? How can we ensure it does not happen again? What were the drivers that led to the situation or the outcome?

My observation is that in most cases there is a genuine and honest desire by the relevant players to achieve the right results and benefits for the organisation. Most always strive to streamline, automate and improve the business of the organisation through the use of IT and, wherever possible, enhance the customer/client experience with the organisation regardless of whether it is public, private or not-for-profit.

So what goes wrong when there is so much goodwill?

ISACA's 40 years of experience in the IT industry confirms that the causal factors for project failures can be sourced back to any point in the project life cycle and can often simply come down to what people/organisations do not know. Valuable tools, methodologies, frameworks, guidelines and briefings highlight the notion that faults can be present in the initial planning stages; the business case development stage; and in any dimension, domain or process during the life cycle of the initiative. Put simply, these are complex undertakings, which require highly skilled and experienced people to diligently manage and lead at all stages from the beginning to end of the initiative. It is evident that managing and leading these changes requires broader

and more comprehensive business experience and acumen than IT. But, so often we expect the IT folks to have all of the answers, skills and experience, while, in more cases than not, this is unfair, inappropriate and not particularly smart. The business changes or reforms enabled by IT take the organisation and the staff to places they have never been before, and frequently no book, guideline or framework can provide the answers to all of the challenges presented. The following are a sample of the challenges faced in this environment:

- Underestimation of the organisational culture or multiple cultures in an organisation by the project team. A disconnect or lack of recognition of the importance of this can often cause a project to be rejected before it has commenced.
- Lack of ownership of the business reform/change by key stakeholders at various levels in the organisation. Capturing the hearts and minds of key informal and formal leaders is a critical success factor.
- Underestimation of the level and complexity associated with the change management affecting people, systems and processes
- Undervaluation of the achievements, rituals, practices and processes of the past and present. So many times the 'baby can be thrown out with the bath water'. Project teams can often become isolated, disconnected and sometimes irrelevant in the medium to longer term if the organisation becomes disconnected, disinterested or disillusioned.
- Underestimation of the inextricable link that needs to exist between the strategy of the organisation (Where are we going?), the structure of the organisation (How will the human, physical and financial resources be organised to achieve the strategy?) and the culture of the organisation (What is important for the people to want to achieve the strategy with the structure provided?)
- Failure to listen to and act upon early warning signs for the project, particularly where the outcomes for the project may be at risk. The use of informal

and formal channels of communication is needed to find out what is really happening or not happening.

- Failure to consult, collaborate, communicate and partner with the organisation to make the reforms/changes become real
- Failure to recognise that the project is a business reform/ change and not an IT initiative. In other words, it could be said that there is no such thing as an IT project, but rather there are business projects that are enabled by IT.
- Underestimation of the need to clearly spell out roles, responsibilities and accountabilities for the business reform/ change. The goal is to never have 'he said, she said; it's his, it's hers; not mine, must be yours; not my problem, must be theirs' conversation.
- Failure to introduce sound enterprise governance of IT. Yes, it is important to have an enterprise approach to govern IT, which is led and informed by the business, not IT.

This is not intended to be an exhaustive list, but rather a sample of many of the challenges that, if not well planned for

and thought through, will see a business reform/change fail regardless of how good it is technically. The list goes some way to confirming a couple of sayings I often use to guide projects: 'It doesn't matter how perfect the technical solution is; if it is not owned and embraced by the business, it will not succeed', or 'Even if the solution is not technically perfect, if it is well implemented, the users will make it work'.

So, where to go from here? In my view, members and constituents of ISACA and the IT Governance Institute (ITGI) are in the best position globally to observe these failures of the past and present. Accordingly, they are also in the best position to influence and change the system into the future with the depth of experience, acumen and a common body of knowledge and through their frameworks and tools including Control Objectives for Information and related Technology (COBIT) and Val IT. However, the solution to the problem is still broader than this.

ISACA/ITGI members and constituents need to advocate not only at every

opportunity and in every forum for the establishment of sound enterprise governance of IT, but also be confident raising many of the cultural, change management and collaborative approaches necessary to make the reforms/ changes happen.

ISACA and ITGI have the frameworks and the broader body of knowledge around enterprise governance of IT. However, our immediate priority is to step up to the challenges listed here—they will make or break projects in the future. While we stop short of these cultural, change management and collaborative approaches, we will continue to see the US \$600 billion per annum failure list grow. Are you equipped, ready and capable to address these challenges?

For more information please visit www.isaca.org

CONTACT INFORMATION

Central Ohio ISACA Chapter
www.isaca-centralohio.org
P.O. Box 151152
Columbus, OH 43215

ISACA International
www.isaca.org
3701 Algonquin Road, Suite 1010
Rolling Meadows, IL 60008 USA
Phone: +1.847.253.1545
Fax: +1.847.253.1443