

China Hong Kong COMMUNIQUÉ

ISSUE 04

Dec 2011

ISACA[®]
Trust in, and value from, information systems
China Hong Kong Chapter

Contents

2 Message from the President/ 会长的话

Chapter News

- 4 2011 ISACA China HK Chapter AGM & Cocktail Reception
- 5 2012 Board of Directors & Committee Members

Membership News

- 9 Highlights of HK Social Networking Event – Poolside Barbeque!
- 10 Co-organize with HKITJC “HKIT Sector Guo Qing & IT Development Class of 2011 at the Tsinghua University”
- 11 Your Director – Simon Chan, the President

Technical Article

- 12 China appears to emerge as a front runner in driving information security initiatives as cyber threats loom large, but still a long way to go

Certification News

- 16 CISA, CISM and CGEIT Certifications Recognized

Academic News

- 17 Our Immediate Past President, Mr. Michael Yung conducted a talk to MBA students of University of Northern Iowa

HQ News & Upcoming Events

- 18 ISACA's World Congress: INSIGHTS 2012

19 Upcoming Events: January – April 2012

20 Quiz of Chapter Newsletter

21 ISACA International and Chapter Contacts



Message from the President

Dear ISACA members and friends,

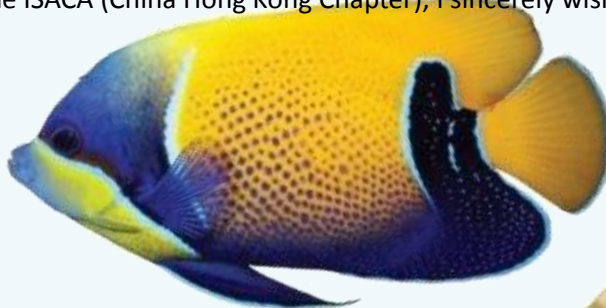
The year of 2011 will soon be over and the new year is fast approaching. ISACA (China Hong Kong Chapter) completed its election of 2012 Board of Directors and Committees at the Annual General Meeting on 8 December 2011. We would continue to devote our wholehearted effort to serving our members. The details of the new directors of the chapter are provided on page 5-7 of this newsletter.

Despite the continuous changes in the world and the volatile economic conditions, the number of members in the chapter has been gradually increasing since its establishment in 1982. In recent years, the China Hong Kong Chapter has become the largest chapter of ISACA. To celebrate the chapter's 30th anniversary in 2012, we have planned to organize a series of activities including the 30th anniversary dinner, IT governance conference, certification training, CPD seminars, social networking events and other professional activities, with a view to enabling our members to share our delight on this important occasion.

We attribute the chapter's success to the professionalism and hard work of all members. Please allow me to show my deepest gratitude to all who have rendered unfailing support to the chapter – Mr. Michael Yung, our immediate past president, all other former presidents, board members, committees, chapter office staff and friends. Without your unwavering dedication, the chapter would not have been as successful as it is now.

Last but not least, on behalf of the ISACA (China Hong Kong Chapter), I sincerely wish everyone all the best. Merry Christmas and Happy New Year!

Regards,
Simon Chan
President
ISACA China Hong Kong Chapter



*In a sea of IT professionals,
ISACA members get noticed.*
www.isaca.org/benefits



会长的话

各位會員及朋友：

2011 年即將過去，新的一年快將來臨。在這送舊迎新、普天同慶之際，國際信息系統審計協會(中國香港分會)已於 2011 年 12 月 8 日 在周年大會上選舉出 2012 年理事會成員和委員，我們將會盡最大的努力，繼續全心服務分會會員。有關本分會新理事的詳情載於本通訊第 5 至 7 頁。

本分會成立於 1982 年，儘管世界變化萬千，經濟環境起伏不定，但在分會各會員同心協力下，會員人數不斷增多，近年中國香港分會已成為 ISACA 全球最大分會。來年將會是本分會成立 30 周年，我們計劃進一步舉辦各項活動，包括 30 周年晚宴、大型研討會、認證培訓、CPD 講座、社交聚會及其他專業活動，從而與各會員朋友分享分會成立 30 周年的喜悅。

分會的發展與壯大，實有賴大家的貢獻及努力。我希望借此機會向剛剛卸任的前任會長翁偉基 (Michael Yung) 先生、歷任會長、理事、委員、分會辦公室同事及所有以往一直支持分會發展的朋友致謝，衷心感謝他們過去的投入及耕耘。他們長期以來的支持實在是分會成功的基石。

最後，僅代表國際資訊系統審計協會(中國香港分會)理事會同仁，向全體會員及業界朋友致以最誠摯的祝福，祝願大家聖誕快樂、新年進步！

陳細明

國際信息系統審計協會(中國香港分會)會長

Chapter News – 2011 ISACA China HK Chapter AGM & Cocktail Reception

ISACA China HK Chapter Annual General Meeting & Cocktail Reception was held at The Hong Kong Bankers Club in Central, Hong Kong on 8 December 2011.

2011 President Mr. Michael Yung reported the activities and the achievements of the Chapter in the past year. And, the new board of directors was elected with full votes. Mr. Simon Chan is the new president and is going to lead the Chapter in 2012.

As an important event of Hong Kong's IT industry, lots of distinguish guests presented in the AGM, including Legislative Council member and the Presidents of the other IT associations.

Written by Mr. Pokit Lok, Newsletter, Committee Member



Photo album of 2011 ISACA China HK Chapter AGM & Cocktail Reception:

<http://www.flickr.com/photos/isacachinahk/sets/7215762834232255/>

Chapter News – 2012 Board of Directors & Committee Members

2012 Board of Directors

Chapter Officers

Position	Name
President	Mr. Simon Chan
Vice-President; Volunteer Coordinator	Mr. William Gee
Vice-President, Secretary	Mr. Victor Tan
Vice-President, Treasurer	Mr. Kenneth Wong
Vice-President, External Affairs	Mr. Raymond Chan
Immediate Past President	Mr. Michael Yung

Board of Directors

Position	Name
Membership (Retention and Development) Director	Mr. Vincent Chan
Membership (Events & Activities) Director	Mr. Sean Lin
Membership (Communication) Director	Mr. Frank Chow
Academic & Student Member Relations Director	Mr. Luke Ma
Co- CISA & CGEIT Coordination Director (HK)	Mr. Michael Huen
	Mr. Wilson Wong
CISM & CRISC Coordination Director (HK)	Mr. Epsilon Ip
Co-Programs Director (HK)	Mr. Patrick Li
	Mr. Ernest Chan

Position	Name
CISA & CISM Coordination Director (North China)	Mr. Samuel Sinn
Co-Professional Development Director (HK)	Mr. Wee Teong Cheah
	Mr. Richard Lam
CISA & CISM Coordination Director (South China)	Mr. Rocky Ho
Professional Development Director (North China)	Mr. Dixon Ho
Publicity & PR Director (HK)	Mr. Peter Koo
Government Relationship Development	Ms. Susanna Chiu
Translation Director	Ms. Jean Wang
Professional Development Director (South China)	Mr. Terence Tang
Professional Development Director (Central China)	Mr. Keith Yuen
Webmaster	Ms. Kobi Chan

If you would like to contact with our Board of Directors, please visit

<http://www.isaca.org.hk/cms/content/view/38/48/>

China Hong Kong COMMUNIQUÉ

2012 Committee Members

Position	Name
Co-Programs, Committee Member (HK)	Diao Tong
	Fung Shek
Webmaster, Committee Member	Chow Sai Hung
	Steven Tsang
CISA & CISM Coordination, Committee Member (Central China)	Cheung Chun Yin
Professional Development, Committee Member (South China)	Frankie Wong
Membership, Committee Member	Harry Ngai
	Rani Lui
CISA & CRISC Coordination, Committee Member (HK)	Rick Cheng
Academic & Student Members Relations Committee Member	Peter Kwan
	Darron Sun
CISM & CRISC Coordination, Committee Member (HK)	Freeman Ng
Newsletter, Committee Member	Dickens Wong
	Pokit Lok
Professional Development, Committee Member (HK)	Jason Ho
Professional Development, Committee Member (North China)	Terence Liu
Professional Development, Committee Member (Central China)	Rajesh Rajagopal
Membership, Committee Member (Central China)	Hong Yonghua
CISA & CISM Coordination, Committee Member (South China)	Tony Chan

Do you know the Chapter is now on...

facebook



新浪认证

flickr®

Eventbrite®

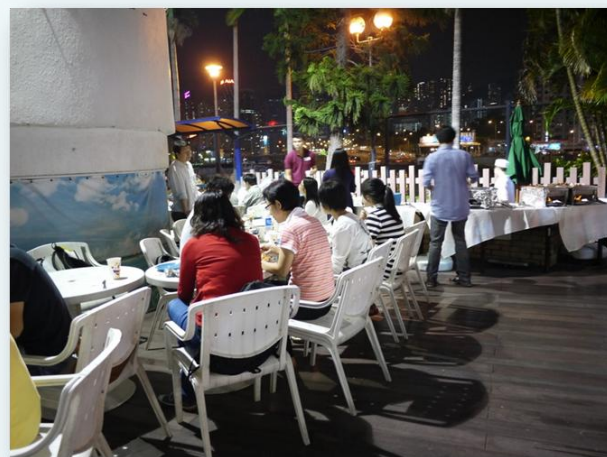
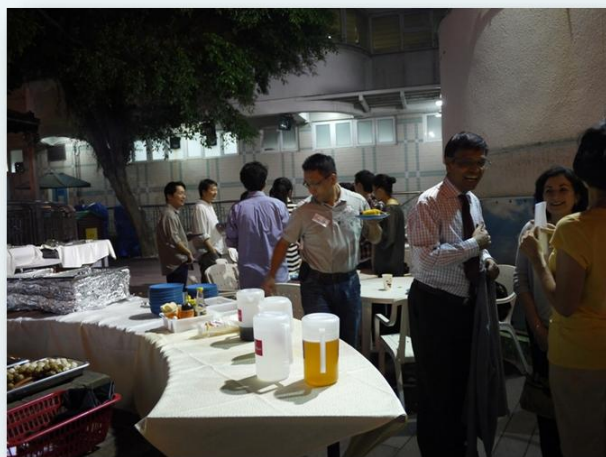
Follow us now!

- | | |
|-------------------|--|
| Eventbrite | http://www.isaca.org.hk/document/20120112_Eventbrite_Instructions.pdf |
| Facebook | Fanpage & Wall : www.facebook.com/group.php?gid=14834061244
Add as Friend: www.facebook.com/profile.php?id=100001489840657 |
| Flickr | www.flickr.com/photos/isacachinahk |
| LinkedIn | hk.linkedin.com/in/isacachinahk |
| Sina Weibo | weibo.com/isacachinahk |
| Twitter | twitter.com/isacachina |

Membership News – Highlights of HK Social Networking Event – Poolside Barbeque!

In the evening of 29 October 2011, over 20 members joined the chapter's Poolside Barbeque. With the beautiful seaview of Victoria Harbour, the members had the nice foods and exchanged the ideas of the latest market and social issues.

Written by Mr. Pokit Lok, Newsletter, Committee Member



Membership News – Co-organize with HKITJC “HKIT Sector Guo Qing & IT Development Class of 2011 at the Tsinghua University”

On 19 – 23 October, 2011, Hong Kong Information Technology Joint Council (ITJC) and the ISACA China Hong Kong Chapter held an HKIT Sector Guo Qing & IT Development Class of 2011 at the Tsinghua University. The Class aims to strengthen understandings of today’s China national conditions, particularly its economic and information technology policies, and facilitate better communication with other industry players.



Your Director – Mr. Simon Chan, President**Mr. Simon Chan****President, ISACA China Hong Kong Chapter**

Simon Chan is the President of ISACA China Hong Kong Chapter, assisting the local chapter in consolidating its position as a leading IT professional body in mainland China and Hong Kong. Simon also hosts activities for the China Hong Kong Chapter, and is committed to enhancing the professional and personal development of the members.



Since 2000, Simon has been actively participating in the activities of ISACA Hong Kong Chapter. Between 2006 and 2011, he has taken up the role of being the Chapter's China Affairs Director and the Vice-President, responsible for promoting information security related professional activities and the association's affair in mainland China and Hong Kong.

With more than 20 years of information system audit related experience, Simon is currently the Deputy General Manager of the Group Audit of Bank of China (Hong Kong) Ltd.

Email contact: president@isaca.org.hk

Technical Article - China appears to emerge as a front runner in driving information security initiatives as cyber threats loom large, but still a long way to go

Source: Kenneth Wong, PricewaterhouseCoopers

To overcome cyber security challenges, organisations need a different mindset to deal with today's cyber security challenges. Kenneth Wong from PricewaterhouseCoopers explains the findings from the 9th annual Global State of Information Security Survey

A new survey study conducted by PwC, in conjunction with CIO and CSO magazines, shows that 61% of Chinese respondents think they have an effective information security strategy in place and are proactively executing their plans, placing them in the category of information security “Front-runners.” 24% of respondents identified themselves as “Strategists” while the remaining identified themselves as “Tacticians” and “Firefighters” (8% and 7% respectively).

The 9th annual global survey of more than 9,600 security executives from 138 countries found that over 70% of global survey respondents report confidence in the effectiveness of their organisation's information security activities - however confidence has declined significantly since 2006. However, the findings of the survey this year have helped carve a new definition of a true information security leader. Even though 61% of Chinese respondents see themselves as front runners which may indicate a false sense of security, according to the survey only a minority of respondents (13%) made the, “leader cut” and they have: i) have an overall information security strategy in place, comprising a proper security governance, organisational structure, security policies and procedures, and roles and responsibilities, and are proactively executing the strategy; ii) a Chief Security Officer (CSO), Chief Information Security Officer (CISO) or executive equivalent who reports to the top of the organisation signifying the importance senior management and board of directors place on information security; iii) a process to measure and review their security policy effectiveness on at least a yearly basis; and iv) a good understanding of the security breaches facing the organisation in the past year. As a result, there appears to be a significant gap (i.e., 61% vs. 13%) between what is perceived by Chinese companies to be sufficient in information security and the reality.

Despite the above finding about Chinese respondents being overly confident in the effectiveness of their information security program, it appears that China has emerged as a front runner in driving information security initiatives due to a number of significant changes in the business and regulatory environment. For example, there has been an increased emphasis on the protection of confidential corporate data, information / data of a national secret nature, and intellectual properties owned by Chinese companies, as well as tougher regulatory data security measures mandated or advocated by a number of senior government officials or supervisory bodies such as the Chinese Banking Regulatory Commission, the State-owned Assets Supervision and Administration Commission of the State Council, etc.

This year, a significant percentage of respondents agreed that one of the most dangerous cyber threats is the Advanced Persistent Threat (APT) attack which usually refers to a group of highly skilled individuals with the capability, resources and intent to persistently and effectively target organisations with high-value information or national critical infrastructure, including national defense, utility, manufacturing, research and the financial services industry. APT is often difficult to be detected and removed and APT intruders have great perseverance and resources to adapt their tools and techniques. APT intruders tend to operate using a “low and slow” approach – stealthily moving from one compromised host to the next, ensuring that their actions cannot be easily detected – to hunt for their specific data or system objectives. The Stuxnet worm is believed to be the first-known worm designed to target real-world infrastructure such as power stations, water plants and industrial units. The Stuxnet worm is believed to have first circulated the World in mid 2009 and was discovered in June 2010 to have infiltrated industrial control systems in Iran to damage the nation's nuclear research program. A new variant, Duqu has been discovered recently with the suspected purpose of gathering intelligence from industrial control systems that can be useful to mount a future attack on an industrial control facility. Similarly organisations in China are exposed to these threats.

This year, significant percentages (83%) of China respondents agree that APT drives their organisation's security spending, yet only 28% say their company has a security policy that addresses APT. So, although China respondents lead their global counterparts, many are not adequately prepared to combat this new threat. APT attacks present different challenges than addressing common computer security breaches, hence, company executives need to be fully aware of the existence and nature of the APTs their companies face and proactively put in place adequate risk assessment and monitoring controls.

According to the survey, the rise of cloud computing has improved but also complicated the security landscape. More than four out of ten global respondents and six out of 10 China respondents report that their organisation uses some kind of cloud computing services. Although 54% of organisations say that cloud technologies have improved security perhaps because of better / easier access to security technologies made available through cloud service providers; while 23% say it has increased vulnerability. The largest perceived risk is the uncertain ability to enforce provider security policies and the lack of transparency on how security is proactively managed by cloud service providers.

While the use of mobile devices and mobile apps represent new opportunities for companies to increase employee productivity and customer interaction, there are significant risks associated with this new tool. In November 2010, The Wall Street Journal cited a research paper quoting a number of data security flaws in leading mobile apps for the iPhone and Android platforms. The paper also cited mobile application holes that left users vulnerable to man-in-the-middle and phishing attacks. Phones were found to be storing sensitive information such as usernames and passwords, account balances, payment records, answers to security questions. Some applications were found to be storing this information in plain text on the phone, requiring little smartphone savvy to access the compromised information. According to the survey, our respondents indicated that security threats targeting mobile devices have increased from 18% in 2010 to 23% in 2010, which underscore the need for e-commerce companies to improve mobile security.

This year social networking, such as Facebook, MySpace, LinkedIn, etc., has emerged as a significant new line of risk. Social engineering, which is the act of using clever lures to trick people into divulging confidential information about their personal lives or the company they work for, is also prevalent on social networks. On social networks, it becomes even easier to exploit trust and launch social engineering attacks. According to the survey, 68% do not have a security policy for social media. This may pose new risks as social networking is increasingly being used by companies, employees and customers.

Managing security risks associated with partners, vendors and suppliers has always been an issue – according to this year's survey it is getting worse. 23% of China respondents identify partners and suppliers as the source of security breaches, up from last year (7%). For years the most commonly suspected source of breaches has been employees, both current and former – and they still are according to this year's survey results. 43% of China respondents identify former and current employees as the source of security breaches, up significantly from last year (11%).

China Hong Kong COMMUNIQUÉ

For several years, Asia (including China), has been firing up its investments in security technology. The number of Asian and Chinese respondents who expect security funding to increase over the next 12 months has leapt to 74% and 83% respectively this year – an expectation rate far higher than any other region. However, despite the optimism in security technology spending, most organisations in China still lag behind in terms of aligning, and getting an appropriate balance between, “people”, “process” and “technology”. The reality is that most Chinese organisations under invest in having regular independent assessment to be conducted to evaluate the operating effectiveness of their security policies and procedures.

The survey findings and the increasing number cyber incident reports we encounter in the media is evident of the increasing cyber security risks organisations face. Collaboration, social networking tools and the increasing use of mobile devices that are currently helping to boost productivity and fuel business growth are also the same tools used by cybercriminals to target vulnerable organisations. The cyber threat landscape is organised, global, highly motivated, sometimes well-funded, patient, and fully immersed in the tradecraft.

When it is discovered, recognition of advanced cyber intrusions does not typically come via in-house technology, processes, or people, but, rather, through third-party tipsters such as domestic law enforcement, intelligence sources, customers, or business partners. It is evident that challenges persist such as where cyber security is still seen as an IT issue, creating a communications gap between managers in the business and the security teams. To overcome cyber security challenges, organisations need a different mindset to deal with today’s cyber security challenges...one that assumes compromise has already occurred and in which cyber forensics is pro-actively employed to detect breach indicators.



Certification News - CISA, CISM and CGEIT Certifications Recognized

This article is extracted from @ISACA Volume22: 26 October 2011

http://www.isaca.org/About-ISACA/-ISACA-Newsletter/Pages/at-ISACA-Volume-22-26-October-2011.aspx?utm_source=informz&utm_medium=email&utm_campaign=informz#4

[ISACA certifications](#) have been recognized by both the National Association of Insurance Companies (NAIC) and Foote Partners LLC. NAIC has included the [Certified Information Systems Auditor \(CISA\)](#) designation among the approved certifications for qualified IT examiners. According to the association, IT examiners must have sufficient knowledge, background and experience to perform the IT portion of a financial exam and CISA satisfies this requirement.

The independent IT research firm Foote Partners LLC's updated [IT Skills and Certification Pay Index](#) found that professionals with the CISA, [Certified Information Security Manager \(CISM\)](#) and [Certified in the Governance of Enterprise IT \(CGEIT\)](#)

designations earn the highest pay premiums among the 53 information security certifications reported in the index. In particular, the CISA credential averages 13 percent of base salary in premium pay and earns between 8 and 11 percent and averages 10 percent of base salary. The average pay premium for all of the certifications reported in the IT Skills and Certification Pay Index is 7.1 percent of base salary.



**Certified Information
Systems Auditor***
An ISACA® Certification



**Certified Information
Security Manager***
An ISACA® Certification



**Certified in the
Governance of
Enterprise IT***
An ISACA® Certification



**Certified in Risk
and Information
Systems Control™**
An ISACA® Certification

Learn more about CISA, CISM, CGEIT, and the Certified in Risk and Information Systems Control (CRISC) designations on the [Certification](#) page of the ISACA web site.

Academic News - Our Immediate Past President, Mr. Michael Yung conducted a talk to MBA students of University of Northern Iowa

On 29 October 2011, our Immediate Past President, Mr. Michael Yung conducted a talk to MBA students from the University of Northern Iowa and the topic was 'Security Enabled Organization'.



The talk was focused on addressing security issues from a managerial perspective and was covered:

- Security in modern day organization
- Safeguarding personal data



Around 20 students attended the talk. The atmosphere of the classroom and response from the students were extremely positive. The students indicated that the view of issues associated with protecting personal data helped in real life. Also, the use of Hong Kong laws and examples gave the presentation a relevant focus for the students.



To have more insight about ISACA student membership, please visit
<http://www.isaca.org/Membership/Student-Membership/Pages/default.aspx>

HQs News & Upcoming Event

ISACA's World Congress: INSIGHTS 2012 is an event unlike any other.

25-27 June 2012 | San Francisco, CA, USA

Designed for progressive IT and business leaders like you, the conference addresses topics at a strategic level, giving you the insights needed to develop strategies for effective integration of business and technology.



INSIGHTS 2012 is:

INSPIRING

You will leave feeling energized, ready to bridge the gap between business and IT after engaging with thought leaders from diverse industries. Through shared experiences, you and your organization will benefit from greater “trust in, and value from, information systems.”

INNOVATIVE

The unique program format revolutionizes the conference experience. From the executive panels, interview sessions and talk-show host format, to the insightful forums designed to address pressing business issues in a more intimate environment, you will gain insights from industry leaders who will facilitate and generate thought-provoking discussions.

INFORMATIVE

This shouldn't come as a surprise, why else would you go to a conference? What sets Insights 2012 apart from other industry events is the caliber of speakers we have selected, in addition to the exciting line up of topics.

For more information about INSIGHTS 2012, please visit

<http://www.isaca.org/Education/Upcoming-Events/Pages/world-congress-2012.aspx>

China Hong Kong COMMUNIQUÉ

Upcoming Events January - April 2012

Date	CPE Hour	Event	Topic/Contents
12 Jan	1	CPD Seminar	Automating Data Discovery, Access Control and Auditing on your Unstructured Data
14 Jan	N/A	Social Networking	Trekking
Feb (TBC)	1	BJ, SH & SZ/GZ - CPD Seminar	To be confirmed
7 Feb	N/A	CISA® & CISM® Briefing Seminars	Introduction of CISA®/CISM® Exams
7 Feb	1	CPD Seminar	To be confirmed
Mar (To be confirmed)	N/A	BJ, SH & SZ - CISA® & CISM® Briefing Seminars	Introduction of CISA®/CISM® Exams
14 Mar	TBC	One- Day Workshop	To be confirmed
15 Mar	TBC	Conference	IT Governance Executive Round Table
16 Mar	TBC	One- Day Workshop	To be confirmed
24 Apr	1	CPD Seminar	To be confirmed

For more information, please visit <http://www.isaca.org.hk>

Office of the Privacy Commissioner for Personal Data, HK (PCPD)

Featured Events: December 2011 - February 2012

1. Free PCPD Data Protection Seminars in December 2011 - February 2012 (in Chinese)

香港个人资料私隐专员公署保护个人资料私隐 -
保护个人资料私隐-日常生活与善用科技讲座系列 (2011年12月至2012年2月)

For more information, please refer the following PCPD web link:

http://www.pcpd.org.hk/tc_chi/activities/promotion.html



香港個人資料私隱專員公署
Office of the Privacy Commissioner
for Personal Data, Hong Kong



Quiz of Chapter Newsletter 分会通信有奖问答游戏

- Q1: Please state the date (Year/Month/Day) of ISACA's World Congress: INSIGHTS 2012
- Q2: Who is the new elected President of ISACA China HK Chapter?
- 请说出 ISACA's World Congress: INSIGHTS 2012 的举办日期(年/月/日)。
- 问 2: 请问新当选为 ISACA 中国香港分会主席是谁?

If you know the answers of the 2 questions, please email your answers of these 2 questions and personal information to info@isaca.org.hk before **13 January 2012**

All winners will receive a souvenir from ISACA China Hong Kong Chapter and will be informed separately. 3 souvenirs are available on first-come-first-served basis.

如果你知道两道题目的答案, 请於 **2012 年 1 月 13 日前**把答案及个人资料电邮至 info@isaca.org.hk。

得奖者将获 ISACA 中国香港分会纪念品一份及获个别通知。名额 3 位, 先到先得。

Knowledge Center



ISACA's Knowledge Center is a networking venue for IT professionals to share common interests.

@ISACA
RELEVANT, TIMELY NEWS

NEW ISACA® Certification—CRISC™



Certified in Risk and Information Systems Control™
An ISACA® Certification

**Grandfathering is now open.
The first exam will take place in 2011.**

Visit www.isaca.org/crisc for more information.

ISACA International Contact

ISACA 总部联络方法

Address:

3701 Algonquin Road, Suite 1010, Rolling Meadows,
IL, 60008 USA

Phone : +1.847.253.1545

Fax : +1.847.253.1443

地址:

3701 Algonquin Road, Suite 1010, Rolling Meadows,
IL, 60008 USA

电话 : +1.847.253.1545

传真 : +1.847.253.1443

Online Feedback Form:

www.isaca.org/About-ISACA/Contact-Us/Pages/Contact-Form.aspx

在线反馈表格:

www.isaca.org/About-ISACA/Contact-Us/Pages/Contact-Form.aspx



Chapter Contact

分会联络方法

ISACA China Hong Kong Chapter

15B, Yam Tze Commercial Building
23 Thomson Road
Wanchai, Hong Kong

Telephone: +852.8101.2801

Fax : +852.8101.2802

E-mail : info@isaca.org.hk

Website : www.isaca.org.hk

国际信息系统审计协会中国香港分会

香港湾仔谭臣道 23 号
王子商业大厦 15 楼 B 室

电话 : +852.8101.2801

传真 : +852.8101.2802

电邮 : info@isaca.org.hk

网址 : www.isaca.org.hk

Office Opening Hours:

Monday 09:00 – 18:00

Tuesday 09:00 – 18:00

Wednesday 09:00 – 18:00

Thursday 09:00 – 18:00

Friday 09:00 – 18:00

Saturday, Sunday & HK Public Holidays Closed

办公时间:

星期一 09:00 – 18:00

星期二 09:00 – 18:00

星期三 09:00 – 18:00

星期四 09:00 – 18:00

星期五 09:00 – 18:00

星期六、星期日及香港公众假期 关闭