

News Brief

Our Chapter Vice President and Newsletter Editor and few other executive committee members of ISACA Jeddah chapter have recently received certifications from the ISACA as Certified Risk and Information Control (CRISC) a new certification.

ISACA UAE Chapter is conducting its Annual Conference 'I-SAFE 2011' from 17 to 19 October 2011. The 2011 event will mark the **Fifth** conference in this very successful education series covering various aspects for managing the most important asset of an organization - **Information**.

This Year's Conference is going to be held @ **The Address Hotel**, Dubai Mall, Sheikh Zayed Road

ISACA, UAE Chapter has lined up a galaxy of international speakers,

including business leaders, security experts and cutting edge IT Governance professionals. There will be unprecedented networking opportunities, 200 regional delegates may participate in this conference.

Register online at www.isacauae.org or contact

Online social networking is major threat to organisations – and it's not just about loss of productivity or bandwidth wastage. Research shows that 90% of all security breaches originate from inside an organisation's ranks. 95% of these breaches are unintentional. So, it is a company's employees who cause most communication and security breaches, and generally they don't mean to.

JEDDAH: A record number of 1,400 Muslims from around the world will perform Haj this year as guests of Custodian of the Two Holy Mosques King Abdullah, Islamic Affairs Minister Saleh Al-Asheikh said Saturday. **MAKKAH:** Makkah Gov. Prince Khaled Al-Faisal said Saturday that the Kingdom would combat all kinds of violations and bad practices during the upcoming Haj such as unauthorized pilgrims squatting on roads, which he said disrupted the movement of legitimate Hajjis. The government has prepared plans aimed at increasing the comfort of pilgrims,

LONDON: The oil industry has an overwhelmingly gloomy economic outlook, expecting recession in the next year, less demand for fuel and lower oil prices, a survey of delegates to a major industry conference showed this week.



Inside this issue:

- Technical Sessions for 2011
- Certification Update
- Journal Update
- Research Update
- Distance Learning Update
- Articles

From the desk of the Newsletter Editor

Fraud is a risk that is always at the bottom of the list of risks for the management as well as for the auditors. The question is that when it is time to promote the fraud risk to a higher level. The answer is that when the red flags are apparent, the risk should be taken into account in the audit plans and as well as control plans of the management. The next question will be that when can we conclude that the red flags merit consideration for the purposes of planning an audit project or enhancing the controls to mitigate fraud risk. If the line management is unwilling to implement the required internal control processes despite the recommendations of the auditors is a red flag and the top management should pay attention to such red flag.

A latest survey of KPMG that compare 2011 with 2007 observations; the survey has revealed that most of the frauds are committed by employees who have been with the organization for over five years and are over the age of 35. The KPMG survey also revealed an astonishing fact that most of the frauds are committed by the Finance Department when there was a firm belief that frauds are committed by the sales department or the purchasing departments. The IT department frauds are at the minimal level.

The Key Objectives: Prevention, Detection, Response

An effective, business-driven fraud risk management approach encompasses controls that have three objectives:

Prevent. Reduce the risk of fraud and misconduct from occurring.

Detect. Discover fraud and misconduct when it occurs.

Respond. Take corrective action and remedy the harm caused by fraud or misconduct.

Pulling It All Together

The challenge for companies is to develop a comprehensive effort to:

Understand all of the various control frameworks and criteria that apply to them.

Categorize risk assessments, codes of conduct, and whistleblower mechanisms into corporate objectives.

Create a broad ranging program that manages and integrates fraud prevention, detection, and response efforts.

An Ongoing Process

Effective fraud risk management provides an organization with tools to manage risk in a manner consistent with regulatory requirements as well as the entity's business needs and marketplace expectations. Such an approach has four phases:

Assess Risks. Identify the scope of the analysis and key stakeholders, profile the current state of fraud risk management, set targets for improvement, and define steps necessary to close the "gap."

Design and develop a broad ranging program that encompasses controls to prevent, detect, and respond to incidents of fraud or misconduct.

Implement. Deploy a strategy and process for implementing the new controls throughout the organization and assign responsibility for leading the overall effort to a senior individual.

Evaluate. Assess existing controls compared with legal and regulatory frameworks as well as leading practices, such as internal investigation protocols or due diligence practices.

Attachments to this issue

- Conference/Training Week Update
- Education Update
- Certification Update
- Membership Benefits

Few delegates who attended our recent event on Disaster Recovery Management



The Executive Committee Monthly Meeting is held on the last Tuesdays of every month.

TECHNICAL SESSIONS CONDUCTED IN 2011

DATE	TOPIC	SPEAKER
Oct 11, 2011	Disaster Recovery Planning Audit & Paragon	Faisal Bashir Mughal
Jun 21, 2011	Application Security and OWASP Top 10	Engr. Amro Al Olaqi
May 24, 2011	Information Assurance Professionals and Virtual Words; Technology's uses, benefits and challenges	Ahmed Faqieh
Apr 26, 2011	Enterprise Architecture	Dr. Adnan Albar
Feb 1, 2011	Business Continuity and Crises Management Workshop	Mr. Dhiraj Lal
Jan 11, 2011	Data Breaches and the next step..	Mr. Paul Wright

** Date and timing of the technical sessions are subject to change based on availability of site and speaker.*



October 05, 2011

A great man died today who made our children to enjoy life with graphics interface. A great man! This earth has seen. All old and young alike are sad to read his death news.

"The world has lost a visionary. And there may be no greater tribute to Steve's success than the fact that much of the world learned of his passing on a device he invented," President Barack Obama said in a statement.

NET WORTH \$7 BLN

Born in San Francisco to a Muslim family of Syria turned Buddhist and raised by US adoptive parents in San Francisco started Apple Computer with friend Steve Wozniak in his parent's garage in 1976. Dropped graduation for a technician job in Olivetti computers. Sold all his belongings to buy equipment to build a workshop in his garage and invented Apple PC. Six years ago, Jobs had talked about how a sense of his mortality was a major driver behind that vision.

Steve Jobs inspiring sayings:

"Remembering that I'll be dead soon is the most important tool I've ever encountered to help me make the big choices in life," Jobs said during a Stanford commencement ceremony in 2005.

"Because almost everything -- all external expectations, all pride, all fear of embarrassment or failure -- these things just fall away in the face of death, leaving only what is truly important."

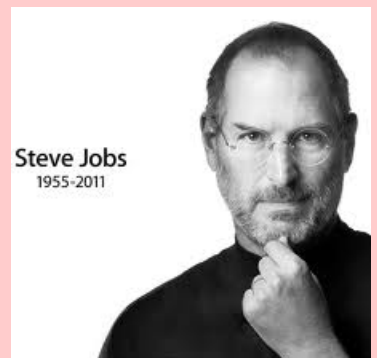
"Remembering that you are going to die is the best way I know to avoid the trap of thinking you have something to lose. You are already naked. There is no reason not to follow your heart."

"For those of us lucky enough to get to work with him, it's been an insanely great honor," said Microsoft's Bill Gates

LEGENDARY ENTREPRENEUR

A college drop-out and the son of adoptive parents, Jobs changed the technology world in the late 1970s, when the Apple II became the first personal computer to gain a wide following. He did it again in 1984 with the Macintosh, which built on the breakthrough technologies developed at Xerox Parc and elsewhere to create the personal computing experience as we know it today.

The rebel streak that's central to his persona got him tossed out of the company in 1985, but he returned in 1997 and after a few years began the rollout of a troika of products -- the iPod, the iPhone and the iPad -- that again upended the established order in major industries.



Articles

Governance in the Cloud

The most frequently used technology phrases in recent history have stemmed from the proliferation of cloud services. Service providers are developing and relabeling services to capitalize on the attention and movement to the cloud as a method to outsource processes, maintain technological advantages and reduce costs. Cloud service offerings have grown exponentially and continue to gain traction because of the promised benefits that cloud computing delivers.

Many companies are now selecting hosting providers that offer infrastructure in the cloud for their customers. These companies reap the benefits of access to advanced technology at a fraction of the cost of making capital investments in dedicated systems. Shared services can deliver improved capabilities to multiple clients who make a shared investment in the technology. However, many of the users of these systems assume that they are outsourcing risk to the cloud as well. I call this "security by abdication." Security by abdication is when a company decides that rather than accept the responsibility of securing and maintaining systems, people or processes, it will abdicate the responsibility by moving to the cloud.

OUTSOURCING RISK?

During an audit, we often hear the phrase, "they handle that." In other words, the company has signed an agreement for Software as a Service or Infrastructure as a Service and breathes a sigh of relief because its responsibility for security on those systems is supposedly in the hands of the service provider. In actuality, the company's responsibility for governing security has not been removed, it is merely different, and must be evaluated in the context of the cloud service, the cloud provider and the purpose for which the company is utilizing the service.

American Health Centers Inc. (AHC) is an example of an organization that chose to outsource its critical infrastructure function, choosing independence IT, a cloud IT vendor. The AHC risk assessment determined that the benefits of hosting data in a secure off-site data center would outweigh the risk of outsourcing management of the systems. It also determined that, given proper governance, security would be improved because the monitoring of access controls provided by independence IT was at a level that AHC would not have been able to provide itself. Security governance is problematic for companies that do not wish to absorb the various matters that must be considered when evaluating risk and managing security. For a company in the business of, for example, producing widgets—and not in the business of securing systems, applications and people—the security function is overwhelming, to say the least.

OVERSEEING SECURITY AND GOVERNANCE

It has been difficult to ask senior executives to oversee a topic with which they are uncomfortable because of the rapid changes taking place with technologies and persistent risks. Governing other departmental goals and objectives is more natural for business leaders and audit committees. Overseeing an information security program that permeates every department and requires a grasp of rapidly transforming subjects has not been as easily adopted.

Many organizations have appointed an information security officer or a different position to oversee the security function and report back to the board of directors. This arrangement has been generally accepted as satisfactory governance even while security incidents are on the rise in the corporate environment.

While governing the risks that it faces, AHC chose to oversee independence IT as a service provider by analyzing its risk management results and audit findings to evaluate the effectiveness of control mechanisms that protect the data and restrict access by unauthorized parties. Whether AHC built and maintained the technology itself or outsourced the capability to independence IT, AHC still has an obligation to govern the information security program that will safeguard patient data.

It is important to note that many organizations' current information security programs do not adequately address outsourced services because the expertise or ability to assess the risks associated with an outsourced provider have not been considered.

CHOOSING A COMPLETE CLOUD VENDOR

The business reasons for choosing a cloud services provider are clear. AHC was able to provide its employees with cutting-edge technology and remote access to applications by using independenceIT's remote desktop client, *Freedom Desktop*, thereby reducing the investment in processing speed and memory requirements. Additionally, the promise of managed security for these remotely accessed systems, applications and data means that the company will not have to monitor, update and test systems on a regular basis, as it would if it were managing all of the systems itself.

However, organizations must consider several other factors when choosing a cloud vendor. Without proper governance of the cloud service provider, an information security program is incomplete, major risks are not considered, and breaches will continue to occur due to misinformation or false expectations placed on the cloud service provider.

Governance of any service provider should include monitoring its risk assessment results to evaluate whether or not its policies and procedures are comprehensive enough to identify threats to its systems, physical locations, employees and vendors. A closer look at a service provider's risk assessment and audit program discloses the matters that should be known by a customer using its services to host and manage sensitive data.

Finally, organizations should also review a vendor's service organization control report because it details the provider's risk assessment process, the controls it has placed in operation and the third-party tests performed to report on operating effectiveness. An organization must accept the responsibility of governing its service providers and what they provide to the company.

CONCLUSION

When outsourcing to a cloud vendor, all of these risks must be evaluated, and governance must be properly implemented, without the assumption that the cloud service is actually doing what it has promised. Due to the rapid expansion and adoption of cloud services, governance is needed more than ever to control and manage the risks.

Joseph Kirkpatrick

ARTICLES

Auditing IT Risk Associated With Change Management and Application Development

Tommie W. Singleton, Ph.D., CISA, CGEIT, CITP, CPA

Using a risk-based approach (RBA) to the IT audit begins with the IT auditor assessing the inherent risk (IR) of the relevant technologies. Some IT risks are generally high, maybe very high, regardless of the industry, type of organization or nature of the individual entity. Some examples of those risks are data transferring between information systems, using a spreadsheet for critical applications and performing customized application development in-house. This article focuses on the last item: change management for custom application development (AppDev).

The next step by the IT auditor is to investigate the control environment to see if the entity has mitigating controls for change management associated with AppDev. The IT auditor needs to assess the control risk (CR) to assess an overall risk associated with AppDev and the audit/review being undertaken. COBIT and other ISACA tools contain a rich set of knowledge and techniques related to this important risk.

This article provides the IT auditor with concepts, techniques, processes and structures that can mitigate the change management risk associated with AppDev. It also provides questions and possible sources of evidence regarding the assurance that mitigating controls could provide.

COBIT AI6 Manage Change

The COBIT 4.1 process associated with AppDev risk is AI6 *Manage change*. This process is described as follows:

All changes, including emergency maintenance and patches, relating to infrastructure and applications within the production environment are formally managed in a controlled manner. Changes are logged, assessed and authorized prior to implementation and reviewed against planned outcomes following the implementation. This process assures mitigation of the risks of negatively impacting the stability or integrity of the production environment.¹

In COBIT, the control objectives related to the Manage change process are:

- AI6.1 *Change standards and procedures*
- AI6.2 *Impact assessment, prioritization and authorization*
- AI6.3 *Emergency changes*
- AI6.4 *Change status tracking and reporting*
- AI6.5 *Change closure and documentation*

These control objectives can be achieved through various practices depending on the capability of the enterprise and the technology involved. One possible set of such practices for AI6 is documented in the *COBIT® Control Practices* publication.² *The IT Assurance Guide: Using COBIT®*² provides auditors with guidance on how to assess the adequacy of their enterprises' design and implementation of their change management processes, based on the COBIT control objective/ control practice content.

Control over the change management process is measured by metrics such as:

- Number of disruptions or data errors caused by inaccurate specifications or incomplete impact assessment
- Amount of application of infrastructure rework caused by inadequate change specifications
- Percent of changes that follow formal change control processes

Other metrics are suggested for consideration in the COBIT AI6

COBIT PO4 DEFINE THE IT PROCESSES, ORGANIZATION AND RELATIONSHIPS

Another way the entity can mitigate AppDev risks is to have a formal structure to deal with some of the previously mentioned responsibilities and accountabilities that enable process activities to occur in a controlled manner (e.g., authorization, prioritization, alignment with business strategy, entity to whom reports are made).

A Steering Committee

COBIT process PO4 *Define the IT processes, organization and relationships* applies to AppDev controls by providing a necessary formal structure. As part of COBIT's Plan and Organize (PO) domain, this process is necessarily about the entity as a whole and the general (management) controls over IT.

PO4.3 provides one of the formal structures that is beneficial to mitigating AppDev risks. According to COBIT 4.1, PO4.3 establishes an IT steering committee (or equivalent) composed of executives, business managers and IT management (i.e., it is cross-functional). Its purpose is to:

- Prioritize IT investments and projects and align them with the enterprise's business strategy and priorities
- Track the status of projects and resolve resource conflicts
- Monitor service levels and service improvements

Other PO4 control objectives such as PO4.5 (*IT organizational structure*) and PO4.6 (*Establishment of roles and responsibilities*) should also be taken into consideration.

As can be seen, these purposes fit the risks and needs to direct and control AppDev. Thus, the IT auditor may want to gather information and evidence about the existence of a steering committee and its operating effectiveness.

An Ideal Structure

Because a steering committee is strategic in nature, and because reporting and tracking of AppDev changes is tactical in nature (i.e., lots of things happen in a week's time and problems need relatively immediate attention), there is a need to consider another level of structure for change control. An ideal structure would be for the BoD to establish a steering committee (or its equivalent) as a cross-functional group responsible for IT projects at the strategic level. This body would, for instance, be responsible for prioritizing and funding IT projects.

But the tactical aspects of AppDev (and other similar IT changes) are probably better suited to a tactical committee that meets more often (probably weekly, but not less than monthly) and is dedicated to solving problems and managing the IT changes hands-on. It may be appropriate for the enterprise to consider using a change management committee to oversee IT-related changes (not just AppDev) from the tactical perspective. The committee should be made up of the business sponsors, representatives of the user groups and the IT function. Tracking the status of changes and resolving conflicts might be better suited at the tactical level than the strategic level (steering committee).

A side benefit of such an organizational approach is that business-unit managers have the opportunity to see changes initiated in other units that have consequences—maybe unintentional—that affect their unit. The change management committee provides the opportunity to vet changes across the business units before certain problems occur.

UPDATES

Delivering Business Benefits With COBIT: An Introduction to COBIT 5

By Derek Oliver, Ph.D., CISA, CISM, CRISC, and John Lainhart, CISA, CISM, CGEIT, CRISC, CIPP/G

COBIT® is an evolutionary framework derived from 15 years of international IT, business, security, risk, assurance and consulting professionals providing their input into what a governance and management framework must provide. COBIT was first introduced in 1996 and has evolved through several major upgrades to its present state, COBIT® 4.1, and the soon-to-be released COBIT® 5.

COBIT 5 is ISACA's newest iteration of its management and governance of enterprise IT (GEIT) framework. It is built on five principles and seven governance enabler models. COBIT 5 is intended for enterprises of all types and sizes. COBIT 5 ties together and reinforces all ISACA knowledge assets, i.e., COBIT 4.1, Val IT™, Risk IT, the Business Model for Information Security™ (BMIS™), the IT Assurance Framework™ (ITAF™), Taking Governance Forward (TGF), and *Board Briefing on IT Governance, 2nd Edition*.



COBIT 5 is designed to deliver business benefits to enterprises, including:

- Increased value creation from use of IT; user satisfaction with IT engagement and services; and compliance with laws, regulations and policies
- The development of a more business-focused IT function
- Increased user contribution to the enterprise

Development Activities

Many volunteers contributed to the design and development of COBIT 5 over the last two years. In addition to the ISACA volunteer leadership groups, the Framework Committee and the COBIT 5 Task Force, volunteers have supported two workshops and have provided subject-matter-expert feedback on the draft products to expand and refine the results to maximise the benefits of the guidance to all IT, business, security, risk, assurance and consulting professionals. The outcome is probably the most significant evolution in the framework since its inception—highlighting the difference between the governance and management activities involved in enterprise IT.

At this point, the framework and supporting guidance are still under development, and to this end, two initial products were made public in June 2011 as exposure drafts to solicit feedback from IT, business, security, risk, assurance and consulting professionals worldwide. Please visit the [COBIT 5](#) page of the ISACA web site to review the initial products and provide feedback.

Following this feedback period and with direction from volunteer leaders, the final touches will put on the COBIT 5 framework material with plans to launch the final products in early 2012. The [COBIT 5](#) web page will be updated regularly with current status information.

Products

The new COBIT 5 presentation and extended guidance will provide IT, business, security, risk, assurance and consulting professionals with a more robust framework for establishing GEIT. The COBIT 5 guidance will initially comprise three products: *The Framework*, *Process Reference Guide* and an implementation guide. The implementation guide will be released in early 2012 with the other two COBIT 5 products. Additional products focusing on particular constituency needs (information security, assurance and risk), enablers (information) and other topics will be planned and developed in the future to support the use of COBIT.

UPDATES

Translation Assistance Available Through ISA-CA

To increase the availability of ISACA® knowledge in non-English languages, which benefits ISACA constituents and the profession as a whole, ISACA offers the Chapter Translation Assistance Program.

Through this program, you can apply for and receive assistance to help your chapter offset the costs of translating ISACA-published material. To qualify, a chapter must submit a business case and receive approval from ISACA prior to commencement of the project or release of funds.

To submit a translation project for consideration, please visit the [Chapter Translation](#) page of the [Chapter Leader Portal](#) and then download, complete and submit the [Business Case Proposal Template](#). It should be sent to Antonio Salzano, ISACA translation manager, by 5 p.m. CST (UTC/GMT - 6 hours) on 9 December 2011 at asalzano@isaca.org. For more information, please download the [Translation Policy Guidelines](#) from the [Chapter Translation](#) page.

CHAPTER SPONSORS



Find ISACA on

<https://twitter.com/#!/ISACANews>

<http://www.facebook.com/ISACAHQ>