Modulo Risk Manager™

Need to increase visibility and proactively gain control of your multi-regulatory compliance and policy management?

New IT and business regulations overburdening your budget and staff?

Is the traditional manual "silied" approach to risk and compliance have you thinking about a standardized and automated GRC management solution?

If you answered YES to any of these questions, contact Modulo today!

THE NEXT GENERATION OF GRC MANAGEMENT IS HERE TODAY!

The Modulo Risk Manager™ solution significantly reduces costs and corporate risk by automating the evidence collection, risk/compliance evaluation, reporting and incident management process for consistent GRC Management. Unlike other build-it-yourself GRC framework solutions, Modulo provides a cost-effective ready-to-use solution with the flexibility to easily customize it to meet your specific requirements.

Contact us
for more information at:
Toll Free 866 663-5802
www.modulo.com

Modulo Solutions for GRC
Governance, Risk and Compliance
25 Years
CPTRAX
Providing Compliance and Control for your Windows® Enterprise.

Automated server-based file change, file security, connection tracking, alerting and control.

Using CPTRAX’s Server Agent technology provides continuous auditing and control to help you protect, respond to compliance requirements, audit and defend your enterprise.

CPTRAX for Windows specializes in providing regulatory compliance reporting to assist with your compliance activities relevant to:

- Sarbanes-Oxley (SOX)
- Payment Card Industry (PCI) compliance
  - Gramm-Leach-Bliley Act (GLBA)
- Health Insurance Portability and Accountability Act (HIPAA)
- Financial Services Authority (FSA)

Use CPTRAX to:

- Audit Kerberos, FTP, NTLM and NTLMSSP Logon + Logoff Activity
- Audit File System Activity for selected folder paths
- Audit Terminal Server and Citrix® Logon + Logoff Activity
- Block undesired file types in selected folders or for your entire file system

CPTRAX for Windows Reports include Workstation Name and IP Address as well as full user account details (SAM, SID, FQDN).

CPTRAX does not use or require Windows® Event Logs.

Download your FREE EVALUATION today!
www.visualclick.com

Visual Click Software, Inc.
PO Box 1497, Austin, TX 78767
Ph: 512-510-4156 - www.visualclick.com
© 2010 Visual Click Software, Inc.
All Rights Reserved.
Information security standards are meant to apply universally. (It is an indicator of our lack of knowledge of astrophysics that we refer to anything that applies everywhere on Planet Earth as being universal.) The best known of these standards are ISO 27001/2, Information technology—Security techniques—Information security management systems—Requirements¹ and Information technology—Security techniques—Code of practice for information security management.² These standards are meant to be applicable to “all [emphasis added] types of organizations (e.g., commercial enterprises, government agencies, nonprofit organizations…).” This International Standard specifies the requirements for establishing, implementing, operating, monitoring, reviewing, maintaining and improving a documented [information security management system] within the context of the organization’s overall business risks.”³

It is questionable whether any standard or, for that matter, any concept of security is applicable to all organizations in all corners of the world, without consideration of national and regional differences. Stated simply, are the perception and the reality of information security the same in Boston, Berlin, Baghdad and Bora Bora? I am not imputing in any way that there are national attributes that would affect security in their countries. But I do believe that there are differences of custom, law, communications, politics and history that make the realization of a Platonic ideal⁴ of information security unachievable.

**CIA**

To complicate matters, there is no globally accepted definition of information security.⁵ A minimal definition, referred to, if not always accepted, is that information security consists of confidentiality, integrity and availability (CIA). While many would argue that there is more to security than CIA, if those three security objectives are not the same everywhere, there is no reason to continue to search for universal meaning in this sphere.

ISO 27001 presents a caveat to universality: “within the context of the organization’s overall business risks.” Thus, one organization in a high-risk field (say banking or the military) might interpret CIA differently from one with lower risk. Clearly, the need for continuous availability in a financial institution in Boston (population 575,000) is greater than that of any organization in Bora Bora⁶ (population 9,000), its economy dominated by tourism. Is the distinction only between the tolerance for downtime in an urban bank and a remote island’s hotels, or is there a real difference in the culture of security in a Polynesian paradise and that of a New England (USA) metropolis? Neither case is provable, but neither can be dismissed, either. Just to admit the possibility of differences cuts into the case for universality.

Data integrity⁷ is an elusive universal goal. Authorized manipulation of data is always affected by who is doing the authorizing and who is doing the manipulating, so that integrity is suspect everywhere, including Berlin and Baghdad. But, one cannot equate the security requirements in peaceful Berlin with those in a city like Baghdad, rent by war. The accuracy and consistency of information are subject to stresses in a war zone that are unlike those elsewhere.

With confidentiality, the C in CIA, we come to the starkest example of a difference in social norms affecting a global consensus on information security. Privacy is a cousin to confidentiality; privacy cannot be accomplished if confidentiality cannot be assured. The weakest control statement in all of ISO 27001/2 deals with this subject: “Data protection and privacy shall be ensured as required in relevant legislation, regulations, and, if applicable, contractual clauses.” Thus, explicitly, there is no universal meaning for privacy—and, by extension, for confidentiality—but rather...
reliance on necessarily local laws, regulations and contracts. In the US, where Boston is located, privacy is limited to industry verticals, primarily financial services and health care. In most of Europe, including Berlin, privacy is a clearly stated fundamental right across society. If C, I and A mean different things in different places, what then is the universality of information security?

SO WHAT?
This is all an interesting philosophical discussion, but what of it? The importance is that multinational companies and those organizations that do business internationally cannot presume that dictates for the security of information resources will be perceived or interpreted in the same way in all locations in which they have interests. The burden is on the management of those organizations to state their own policy, standards and procedures and not simply to adopt international standards, i.e., ISO 27001/2, as their own.

Moreover, consistent metrics are needed to assess compliance with those organizations’ standards. Measurement of the effectiveness of security has long been a conundrum; the absence of breaches is not necessarily indicative of the presence of security. With access to an organization’s databases available globally, information security is no better than the implementation of standards wherever the interpretation of those standards is the most lax.

With regard to ISO 27002, compliance is measured through the process of certification described in ISO 27001. The closest equivalent for measuring compliance with an organization’s own standards is the audit process. Still, auditors live within their social milieu. Audit independence implies that the auditor is not personally involved with the controls. Independence cannot assure that two auditors, one in Boston and the other in Baghdad, will look at the same implementation of security and reach the same conclusions. They are human and work within their own personal and societal biases.

CULTURAL BIAS
Since the ISO standards were also crafted by human beings, are there cultural biases embedded in them? ISO 27001/2 was derived from a British standard. Although there have been major improvements to the standards over time, there are still significant passages from BS 7799 that appear in ISO 27002. The original was written by a committee of Britons, some of whom are personal acquaintances. Fine fellows all, but they could not help but see the world, and the security of the information in that world, through the lens of the society in which they were raised and live. It is a testament to their work that it has resonated with so many people in such far-flung places for so long.

International security standards imply a global consensus on the meaning of security—one that is not clear, for example, between democracies and dictatorships, large and small economies, or so-called first- and third-world nations. Governments prefer security standards so that they can enforce uniformity within their jurisdictions. Unfortunately, they are not quite so fond of standards emanating from other jurisdictions. In the private sector, the need for consistency in global affairs works against national standards. The inherent dialectic between localism and universality is, as I have been saying, unresolved.

The more generic international standards are, the less “standard” they are in implementation. The more prescriptive they are, the more difficult it is to make them work in specific instances. Security standards are established to deal with a wide range of potential exposures; a given organization may not need to address them all. Moreover, the funding required for broad-based adoption of security standards may work against achievement of any standardization. If universality of information security standards is ultimately an unattainable goal, organizations should seek to impose, monitor and audit compliance with those of their own making.

ENDNOTES
3 Op cit, ISO 27001, p. 1
4 The Greek philosopher Plato described a dual reality, that of the material world and the transcendent realm of forms. Thus, for the purposes of information security, there is security as we find it in the world we perceive and an ultimate, universal expression of security. This duality has been argued through the centuries. The philosophic
issue is whether a universally applicable concept of information security can be separated from the world as we experience it.

5 I have discussed this question in a previous ISACA Journal column, “IS Security Matters?,” vol. 2, 2010.
6 No slight intended to the good people of Bora Bora, but the alliteration does lend itself to its choice as a representative small nation.
7 Defined as “accuracy and consistency of stored data, indicated by an absence of any alteration in data between two updates of a data record,” Business Dictionary, www.businessdictionary.com/definition/data-integrity.html
8 US Congress, Financial Services Modernization Act, (better known as the Gramm-Leach-Bliley Act), USA, 1999
9 US Congress, Health Insurance Portability and Accountability Act (HIPAA), USA, 1996
11 British Standards Institute, BS 7799, 1995. In fact, the ISO standards still retain codedesignation as BS 7799.

The Risks and Rewards of Cloud Computing

Do the risks outweigh the benefits?

Realizing the business benefits of this emerging technology, with security, governance and assurance perspectives.

www.isaca.org/cloud
Top Five Fraud Axioms IT Auditors Should Know

Somewhere in the career of the IT auditor, he/she will come across a piece of evidence of a fraud (and possibly not realize it is related to a fraud), discover a fraud or be asked to assist in a fraud investigation. Thus, one of the basic sets of knowledge the IT auditor needs is some essential information about fraud detection. This article attempts to identify some of the most important facts about fraud that are particularly applicable to the IT audit function. It is not intended to be an exhaustive list, but rather five things that would assist IT auditors in fulfilling their duties related to fraud in everyday tasks. These five are not ranked in any particular order.

1. PROFESSIONAL SKEPTICISM
One of the first things with which IT auditors need to get comfortable is the realistic view of the scope of fraud. According to the Association of Certified Fraud Examiners (ACFE), the total loss from fraud in any one year in the US is between 5 and 7 percent of gross revenues, with the latest statistic estimating total losses in the US economy at almost US $1 billion.1 One element of fraud that seems to occur frequently is the shock from the victim’s stakeholders that it happened to their entity. These facts are raison d’être for an antifraud program and/or fraud audit for any entity. So, the conclusion is twofold: Fraud has a vast scope, and it can happen anywhere. Therefore, it is important to be consistent with professional skepticism.

Also, the fraudster (white-collar criminal) is usually someone that is least suspected. In fact, fraudsters frequently do not look like crooks at all. Statistical profiles of white-collar criminals describe them as tending to be tenured at the entity, in a trusted position because they earned the trust of management, and relatively well educated.2 Again, professional skepticism is necessary to prevent one from being fooled, and, even then, there is a chance a fraudster can get away with a crime.

2. TOE IN THE WATER
One theory of fraud suggests that fraudsters begin their slippery slope into crime with a “test.”3 That is, they put together a fraudulent transaction or event and “float” it out into the entity’s environment to see if they can get away with the fraud. If that first instance gets noticed, the fraudster usually has a predetermined “excuse” for why it happened, often the “oops, I made a mistake” defense. If it goes unnoticed, the fraudster usually proceeds to the third item in this list.

The IT auditor needs to be aware that if he/she finds an unexplained anomaly or variance, and goes to the party responsible, and that person says “oops,” there is some probability, no matter how small, that it is a “test” transaction. The IT auditor should exercise due diligence in obtaining independent verification where feasible and should obtain it before approaching the party responsible for the transaction, where feasible—especially where circumstances increase suspicion. For example, in one fraud case, the auditor came to the responsible party and asked why a certain account amount was exactly double what it should have been. The accounting clerk stuttered, having been surprised, and the auditor himself gave the person an opportunity to use the “oops” defense, as he said to her, “You must have accidentally double paid the vendor.” In reality, it was a fraud scheme and not an overpayment.

3. ESCALATION OF THE CRIME
Most fraudsters who get caught tend to escalate their crime. This is substantiatted by a variety of facts. ACFE’s regular Report to the Nation (RTTN), published in 1996, 2002, 2004, 2006 and 2008 (the 2010 version is currently being conducted), shows that, of the three main categories of fraud, there is an overlap in percentages because fraudsters were conducting frauds in more than one broad category. In one year, more than 4 percent of all frauds discovered and resolved included asset misappropriation, corruption and financial statement schemes by the fraudster.
Thus, the fraudster who floats the test and finds that it goes unnoticed will decide to take more from the victim. That can be done by committing more fraudulent transactions in a shorter period of time, taking larger amounts in each transaction or adding a new scheme. Again, this applies to fraudsters who get caught, as no statistics exist for frauds that go undiscovered. But, this escalation is good news to those looking for evidence of fraud because it makes it easier to discover. Therefore, the IT auditor should remember this fact when performing data mining activities. For instance, a trend analysis by a vendor that shows a significant increase in purchases over time might be a red flag associated with an escalation of a kickback scheme, shell vendor or other vendor-related scheme. The same could be said about other analytical procedures and accounts or classes of transactions.

For example, in one famous financial statement fraud, the senior executives started out in 1986 with a simple scheme to increase net income by about US $50,000. They worked hard to fool the auditors and managed to do so for more than a decade. By 2001, there were several schemes for that year, and a batch of fictitious journal entries of more than US $7 million alone.

4. TIP OF THE ICEBERG

Many times, a fraud is discovered by accident rather than as a result of deliberate procedures. In such cases, usually an astute auditor looked at a single event or transaction (e.g., a check for US $2,000), became suspicious for one reason or another (often described by experts as “the smell test”), and chose to dig deeper (e.g., to find dozens of other checks totaling US $400,000 and another fraud scheme). This is the “tip of the iceberg” theory. The first check was insignificant in the amount, but if it is part of a sample, or one line of data in an accounting file, it could be just one of many fraudulent transactions. That is, when an anomaly comes to the attention of the auditor, the auditor should stop and think about the probability that this single anomaly is stand-alone or the visible part of an “iceberg,” in which case the preponderance of the mass is under water and out of sight. For instance, if the IT auditor notices in the data that an employee received two checks in one pay period for the same gross amount and corporate policy does not allow for more than one check per pay period, that circumstance would be an anomaly (a red flag). Someone may provide a legitimate-sounding reason for the duplication (“oops”), but the IT auditor should consider drilling down on those facts to see if more fraud and/or suspicious data exist.

This concept extends into the discovery of the fraudster. It is fairly common for a fraudster who gets caught and chooses to confess, to confess to the amount of fraud known up to that point, or some amount that is far below the actual amount (i.e., confesses to the tip of the iceberg or some amount significantly less than the whole iceberg). Obviously, the fraudster is hoping the victim will stop looking and deal with the lesser amount. For example, the fraudster may decide it is easier to confess to US $30,000 and pay it back, than to admit to the actual US $400,000 fraud. Thus, the IT auditor and fraud investigation team should consider a thorough fraud audit to determine the amount of loss independent of the fraudster, to the degree practicable. That subsequent fraud audit is likely to benefit from data mining and data analysis by the IT auditor.

5. DATA MINING AND ANALYSIS

Generally speaking, data can be invaluable in a fraud investigation. Proper data mining and data analysis can lead to a proper description of the fraud, how it took place, what controls were thwarted, the approximate level of loss and even who committed the fraud. So the IT auditor can play an invaluable role in gathering data, mining it, analyzing it, and providing the lead investigator with evidence and information. Also, the IT auditor can be an invaluable resource to convert the mass of data into something that a judge or members of a jury can easily understand and assimilate into their thought processes (e.g., charts, diagrams, other high-tech visual aids).

But, usually, the data alone are insufficient to make a case, even if it is a corporate investigation. A court case will likely require more than just the data. Therefore, the IT auditor needs to work closely with the lead investigator and others on the investigation team, as the team will likely need to conduct interviews and perform other tasks to collect more evidence and information.
CONCLUSION
The IT auditor has a key role in fraud detection, prevention and investigation in today’s business world. It is important for the IT auditor to understand the key aspects of antifraud as it relates to IT audit. This knowledge could help the IT auditor be prepared to recognize a piece of fraud evidence, develop a sense of red flags and understand how certain fraud schemes are perpetrated. These five issues are a start in developing the knowledge and skills to be effective at detecting and investigating frauds.

ENDNOTE
1 The ACFE’s Report to the Nation is a regular report on fraud in the US. In the 1996, 2002 and 2004 reports, experts estimated fraud losses at 6 percent; in 2006, it was estimated at 5 percent; and, in 2008, it was estimated at 7 percent.
2 Ibid.
3 Based on the author’s experiences and the first-hand accounts of fraudsters such as Sam Antar (Crazy Eddie’s fraud) and Bill Owens (HealthSouth fraud).
Five Questions With...

William R. Stanek

William R. Stanek (www.williamstanek.com) is a leading technology expert, an award-winning author and an instructional trainer. As the author of more than 100 books, his practical advice has helped millions of readers all over the world. His books include Exchange Server 2010 Administrator’s Pocket Consultant, Windows PowerShell 2.0 Administrator’s Pocket Consultant and Windows Server 2008 Inside Out. In addition to his IT-related works, Stanek is an accomplished fiction writer of comic books, graphic novels and children’s books.

Stanek recently rediscovered his love of the great outdoors. When he’s not writing, teaching or making presentations, he can be found hiking, biking, backpacking, traveling and/or trekking in search of adventure.

Follow Stanek on Twitter at twitter.com/WilliamStanek.

Q How do you think the role of the IT auditor/professional is changing or has changed? What would be your best piece of advice for IT auditors as they plan their career path and look at the future of IT auditing?

A Anyone working as an IT auditor/IT security professional today had best be ready for a ride. Change is happening in the industry and more changes are inevitable. Government regulation and compliance requirements are increasing and likely will continue to do so. Continued reform and revisions to existing guidance that closer approximate reality must come, and the professionals working in IT security and auditing should be the driving forces behind these changes (rather than waiting for change to happen). IT security is an ongoing continuous concern; IT security policies and IT auditing practices need to be ongoing and continuous as well.

In the US, government agencies (and some other organizations) use Federal Information Security Management Act (FISMA) guidance to aid in their security practices and help establish baseline guidance. Widespread reform of FISMA is needed to close the gap between what is perceived and what is real. Certification and accreditation are parts of a larger whole and must be seen as such. Achieving compliance with National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 controls is a start, but compliance must be backed by enforcement and penalties for lack of enforcement, as well as by expanded guidance beyond the minimum requirements provided in NIST SP 800-53.

Q How do you see the role of governance of IT changing in the next five years?

A In the past, change in security standards and practices happened rather slowly. Well, it is catch-up time, and over the next five years, the role of IT governance will grow markedly as organizations large and small increasingly adopt IT governance, risk and compliance guidelines to keep pace with the rapid changes in the real world.

This whole notion of governance of IT is expanding and only will continue to do so. IT must support and enable an organization’s strategies and objectives. Otherwise, IT is an impediment to the organization’s success.

ISO/IEC 38500, Corporate governance of information technology, provides good guidance on better aligning IT with organizational decisions, but a standard is only a starting point. Beyond such, standards are recognized frameworks that are continuing to evolve and change as our understanding of what IT governance, risk and compliance must entail evolves and changes.

IT governance frameworks such as COBIT® and Val IT™ provide the strategic concepts and tactical principles, and operational frameworks such as Microsoft Operations Framework (MOF) and IT Infrastructure Library (ITIL) define...
best practices for IT service management and support in operational environments. All of these policies and guidelines are meaningless if they are not current with the times and actual needs—and this is why the role of IT governance must expand and adapt, becoming more proactive and responsive.

Q How do you see information management practices in business changing in the short and long term? What are the biggest concerns with cloud computing, and how do you see them being addressed?

A Information management practices increasingly must focus on data governance. Proper data governance helps an organization better manage, protect and use the intellectual property and other data in its possession. In the short term, an increasing focus on data governance likely will require ongoing changes to information management policies, and those ongoing changes must then be implemented in increasingly wider scope while ensuring that privacy, confidentiality and compliance needs are met. In the long term, fully aligned data governance, risk management and compliance objectives must become a core focus and a way of doing business.

Increasing adoption of cloud computing will make this increasing focus on data governance a challenge, and a balance will need to be found between the way data are governed internally and externally. Successful IT organizations will identify, analyze and evaluate the risks of outsourcing infrastructure/services and storing data in the cloud and then implement policies to mitigate, remedy and monitor those risks. My biggest concern is that a strong balance between transferred risk management and internal risk management will need to be found. Some risk management tasks may be best performed by cloud service providers themselves and others by internal teams. If the proper balance is not found and maintained with excellent oversight, the organization may put itself and its future at risk.

Q How do you balance your careers as an IT professional and fiction writer? Do you use your experiences as an IT professional when writing fiction? How do the two careers converge?

A I work hard every day to balance my careers as both an IT professional and a fiction writer. Working in IT, especially with my focus on new and emerging technologies, gives me excellent insights into the ways complex processes and environments should be managed. Writing a work of fiction, such as my latest release, *Rise of the Fallen* (*Ruin Mist: Dawn of the Ages, Book 1*), is itself a complex process that requires excellent management to carry the project through to completion. My many years of managing and writing about complex systems as an IT professional have made it easier for me to write about complex worlds and societies in my fiction. My experiences as an IT professional also enable me to work comfortably in every aspect of the writing and production processes. So, not only did I write the *Bugville Critters* picture books for children, I also rendered and finalized the art and did the layout. For my upcoming comic books, including *Betrayal* (*A Daughter of Kings, Comic #1*), and the related graphic novels, I wrote the scripts, rendered and finalized the art, and lettered the works in their entirety. The result, I think, is a tighter, more cohesive product.

The IT and fiction careers converge in many other ways as well. For example, I developed the digital production processes used by my fiction publisher at a time when most other publishers were nondigital, and I continue to evolve these processes. These digital processes allow the publisher to more easily produce my work in the many forms and formats needed in this increasingly complex digital age.

From time to time, I also sneak technology into my writing. For example, *Pieces of the Puzzle* is, on the surface, a thriller about agent Scott Evers who is forced to go rogue to clear his name. Rippling under the surface is the story of the machines that control the world’s financial networks and the cautionary tale of how tampering with those machines propels the world into financial chaos.

Q What has been your biggest workplace challenge, and how did you face it?

A My biggest workplace challenge has always been one of reversing negative perceptions about IT. It seems every time a company I work or consult for gets new managers outside of IT, the new managers come in with a negative perception of IT. They seem to think IT exists only to put up roadblocks and hinder progress, when this is not true in a well-run IT organization. Great IT organizations are the beating heart of any business, and like any well-oiled engine, IT should be seen as the doer who gets things working and keeps them working, all while performing the Herculean feat of ensuring governance, risk management and compliance objectives are met.
There have been articles in the mainstream media discussing efforts by technology companies and providers to digitize patient records. There is a tremendous push by the US federal government—as well as by some private payers and self-insured employers—to get all US health care providers wired in the near future, in an effort to better coordinate patient care, improve outcomes and “bend the cost curve” all at the same time.

Once patient data, known as protected health information (PHI), are stored electronically, they become exposed to potential data breaches. There are two pieces of recent legislation issued by the US Congress that affect, more than any other recent legislation, the security and privacy areas reviewed by IT auditors in the health care industry:

1. **Health Information Technology for Economic and Clinical Health (HITECH) Act**

This article will address the HITECH Act. A second article, publishing in volume 5, 2010, of the *ISACA Journal*, will address HHS BNR.

Compliance with both of these rules—issued under authority of the HITECH Act by the HHS with respect to health care providers and by the US Federal Trade Commission (FTC) with respect to electronic health care record (EHR) vendors and other similar third parties—requires affected practices and businesses to assess and update their data privacy and security policies and procedures, as well as train all affected staff accordingly.

The HITECH Act was signed into law in February 2009 as part of the ARRA. The HITECH Act:

- Includes goals related to the use and security of electronic health records to improve quality of care and reduce health care costs
- Charges the Office of National Coordinator for Health Information Technology (ONC), a division within HHS, with coordinating efforts to implement HITECH Act requirements, including establishing national standards related to use and security of electronic health records
- Strengthens enforcement and penalties associated with willful violations of US Health Insurance Portability and Accountability Act (HIPAA) requirements, such as disclosure of PHI, and provides requirements for notifying affected individuals when PHI has been, or is reasonably believed to have been, disclosed as the result of a breach

This article will briefly describe the HITECH Act and its impact on IT professionals in terms of:

- What is this piece of legislation? Who is covered under this legislation?
- When is it applicable? Do all organizations have to start complying with the legislation immediately?
- Who needs to follow/implement this legislation?
- What do organizations have to do to comply with the legislation?
- Why do IT auditors need to know about this legislation?
- What do IT auditors need to know about it? What is the role of IT auditors? Is it checking compliance at the end of a period/year, or is it a continual process?
- What are the applicable fines or effects if these rules/acts are not followed?

**THE HITECH ACT AND WHO IT COVERS**

On 17 April 2009, HHS issued guidance specifying the technologies and methodologies that render protected health information unusable, unreadable or indecipherable to unauthorized individuals, as required by the HITECH Act, passed as part of the 2009 ARRA.
This guidance was developed through a joint effort by the Office of Civil Rights (OCR), the ONC and the Centers for Medicare and Medicaid Services (CMS). The HITECH Act and its implementing regulations became effective in the fourth quarter of 2009. Auditors and security professionals need to understand this Act and its implementing regulations because they significantly expand the HIPAA security and privacy requirements. Similar breach notification provisions implemented and enforced by the FTC apply to vendors of personal health records and their third-party service providers, pursuant to section 13407 of the HITECH Act.

The HITECH Act has led to the first breach notification requirements in the US. Under the Act, a breach is defined as the unauthorized acquisition, use or disclosure of PHI. Organizations are exempt from the breach notification requirements if they can demonstrate that disclosures do not compromise the security or privacy of the data or lead to a significant risk of harm to affected individuals.

The HITECH Act directed the secretary of HHS to issue technical guidelines to health care providers. Published in August 2009, this guidance:

- Requires health care providers and other HIPAA-covered entities to promptly notify affected individuals of a breach
- Mandates notification to HHS and the media in cases where a breach affects more than 500 individuals. Breaches affecting fewer than 500 individuals must be reported to the HHS secretary annually. Guidance drafted by HHS extends to business associates of health care providers as well. The FTC has issued companion breach notification regulations for vendors of personal health records and other entities not covered by HIPAA. It should be noted that this affects non-US based companies that do business in the US or with US companies.

Under the HHS and FTC regulations, notification is required when information is unsecured. These regulations specify encryption and destruction as the technologies and methodologies that render PHI unusable, unreadable or indecipherable to unauthorized individuals. Entities that secure PHI in accordance with the regulations are relieved from having to notify individuals, the HHS secretary and the news media in the event of a breach. The breach notification regulations became effective in September 2009.

**COMPLIANCE DEADLINES**

Interim final breach notification regulations, issued in August 2009, implement section 13402 of the HITECH Act by requiring HIPAA-covered entities and their business associates, including those based outside the US, to provide notification following a breach of unsecured PHI. The HHS reports that similar breach notification provisions, implemented and enforced by the FTC, apply to vendors of personal health records and their third-party service providers, as specified in section 13407 of the HITECH Act. Section 164.400 of the interim final rule provides that this breach notification rule is applicable to breaches occurring on or after 30 days from the date of publication of this interim final rule, August 2009.

**WHO IS COVERED UNDER THIS LEGISLATION AND WHO NEEDS TO FOLLOW IT?**

The legislation indicates that the breach notification rules apply to covered entities under HIPAA and their business associates and require them to provide notification in the case of breaches of unsecured PHI. The Act also requires covered entities to provide to the media notification of breaches. The Act requires covered entities to safeguard electronic PHI and permits covered entities to use any security measures that allow them to reasonably and appropriately implement all safeguard requirements.

The HITECH Act applies to both vendors of personal health records that provide online repositories that people can use to keep track of their health information and entities that offer third-party applications for personal health records. These applications could include, for example, devices such as blood pressure cuffs or pedometers whose readings consumers can upload into their personal health records. Consumers may benefit by using these innovations, but only if they are confident that their health information is secure and confidential.

**COMPLYING WITH THE LEGISLATION**

Organizations have to do the following to comply with the HITECH Act:

- Implement a data classification policy—approved by senior management and communicated by management—that
describes the acceptable processes used to identify, classify, store, secure and monitor access to a consumer’s PHI data.

- Implement a process to detect a potential data breach and initiate timely incident response activities.
- Implement a notification process. Vendors and related entities with access to personal health records need to ensure that a process is in place to notify affected parties without unreasonable delay and no later than 60 calendar days after discovery of the breach of the security of their individually identifiable health information. The rule specifies that notifications should:
  - Be written in plain language
  - Include, to the extent possible, a brief description of what happened, the types of information involved and steps individuals should take to protect themselves
  - Include a brief description of what the entity is doing to investigate and mitigate the breach. The notification must provide consumers with contact information that includes a toll-free number, e-mail address, and web site or postal address.
- Implement processes, policies and procedures governing its training program, and report and file complaints to ensure compliance. Limited guidance has been issued to date defining minimum requirements for compliance.
- Encrypt data—at rest and in transit. Since data are a company’s most valuable asset, compromise, disclosure or alteration could have a significant negative impact. Generally, encryption methods such as the Data Encryption Standard (DES), Blowfish, RSA (which stands for Rivest, Shamir and Adleman, who first publicly described it), RC5 (Rivest Cipher) and International Data Encryption Algorithm (IDEA) are used as the basis for implementing encryption technologies. In addition to servers and desktop workstations, encryption must be implemented on portable devices, such as laptops. A process for determining the business rationale and approval for encrypting the data at rest or in transit is needed to ensure the encryption effort is effectively implemented. Electronic PHI has been encrypted, as specified in the HIPAA Security Rule, by “the use of an algorithmic process to transform data into forms in which there is a low probability of assigning meaning without use of a confidential process or key” and when such confidential process or key that might enable decryption has not been breached. The US National Institute of Standards and Technology (NIST) tests encryption methodologies and identifies those that meet applicable standards.

RESULTS OF NONCOMPLIANCE

The secretary of HHS is responsible for oversight, enforcing compliance and determining the amount of any proposed penalty.

WHY DO IT AUDITORS NEED TO KNOW ABOUT THE HITECH ACT?

IT auditors need to know about this regulation because the interim final rule for the HITECH Act, which was issued in April 2009, states that a breach does not occur unless the access, use or disclosure poses “a significant risk of financial, reputational or other harm to an individual.” In the event of a breach, the rule requires covered entities to perform a risk assessment to determine if the harm standard is met. If risk assessment determines that the risk of harm to the individual is not significant, the covered entities are not required to tell their patients that their sensitive health information was breached. The FTC version stipulates that if an individual authorized the discharge of data, the data’s release is not considered a breach. The final rule became effective during August 2009.1

The FTC’s rule also allows for a vendor to engage in a risk analysis and states that if data were never acquired (i.e., officials are fairly certain that nobody saw the material), the incident does not count as a breach and notification does not have to occur. Both agencies have said they will not enforce the data breach rules for 180 days, during which time Devon McGraw, director of the health privacy project at the Center for Disease and Technology (CDT), hopes that HHS will go back to the drawing board.2 With regard to the possible overlap with state regulations specifically over the definition of breach notification, at this time, it appears any US state law is preempted. Auditors employed by a multinational firm or an organization with offices in multiple states will have to take this added complexity into consideration when assessing the organization’s compliance.

The HITECH Act also provides guidance and funding for establishing at least 70 regional centers to help promote EHR adoption. Practice Fusion, a newsletter for physicians, indicated earlier in 2010 that regional centers will offer “technical assistance, guidance and information on best practices to support and accelerate health care providers’ efforts to become meaningful users of EHRs.”3 More than 100,000 primary care providers will be supported by the regional centers. An excerpt from a Health Information Technology Extension Program: Regional Centers...
Cooperative Agreement Program document says that support should specifically focus on helping providers select the highest-value option, defined as that which offers the greatest opportunity to achieve and maintain meaningful use of EHRs and improved quality of care at the most favorable cost of ownership and operation, including both the initial acquisition of the technology, cost of implementation, and ongoing maintenance and predictable needed upgrades over time.4

Under the HITECH Act Medicare and Medicaid bonus payouts, a physician who can demonstrate “meaningful use” of an EMR in 2011 would be eligible to receive US $18,000 from Medicare for the first year and US $44,000 total through 2015. Incentives are reduced for adoption after 2012. Physicians whose practices feature a high volume of Medicaid patients can qualify for up to US $65,000 in incentives.

REFERENCES
Federal Register, Part II, Department of Health and Human Services, 45 CFR Parts 160 and 164, “Breach Notification for Unsecured Protected Health Information; Interim Final Rule,” USA, 2009
IT Governance Institute, COBIT 4.1, USA, 2007
Department of Health and Human Services, Health Information Privacy, HIPAA Administrative Simplification Statute and Rules, USA, December 2000

ENDNOTES
1 According to Devon McGraw, director of the health privacy project at CDT, the language was not handed down as part of the US $19 billion health IT section of the economic stimulus package and was expressly rejected by House of Representative staffers who helped craft the measure. He noted its inclusion by HHS is likely the result of lobbying on the part of the health care industry. CDT and its allies favor the approach taken by the FTC in its own data breach mandate, which takes effect the same day as the HHS rule.
Noyes, Andrew; “HHS Urged to Rework Data Breach Rule,” Congress Daily, Tech Dose Daily, 17 September 2009
2 Ibid.
4 Health Information Technology Extension Program: Regional Centers Cooperative Agreement Program, “Funding Opportunity Announcement and Grant Application Instructions,” Office of the National Coordinator for Health Information Technology Department of Health and Human Services, USA, 2009
GOOD FORTUNE
Can Be Yours

BREAK INTO IT.
Register for an ISACA certification exam.

Exam Date: 11 December 2010
Registration Deadline: 6 October 2010

www.isaca.org/certification
The IT industry has been witnessing an accelerated rate of security breaches in the rapidly expanding technologies. Yesterday’s solutions may be stale or may act as guidelines. Today’s solutions may be strategies only for survival. Solutions for tomorrow’s unknown risks may be uncertain, but would need guidelines to ensure security and privacy to the best of abilities. This book serves as a reference for information security and privacy professionals.

The book takes the approach of examining and questioning the current and traditional approaches to determine their strengths and weaknesses and to suggest paths forward that will overcome their deficiencies.

To meet the objectives of this book, 19 authors were chosen who have strong practical backgrounds and who have succeeded in providing recommendations that are realistic, visionary and doable in the rapidly changing technical and social worlds.

Three editors contributed in two different ways. The editors have included their own comments in each chapter to stimulate thought and discussion. They encouraged authors’ creative thinking and presentation based on their backgrounds—leading to certain differences in referencing formats, but with no significant impact on content.

This book is organized into three parts and contains 13 chapters, followed by an appendix. Every page has footnotes with references to chapters of books, articles of journals and web pages.

Part I, Trends, traces the history of security, privacy and information technology. It contains five chapters. Each chapter is organized by background, observations, recommendations and future trends. The chapters in this section address data classification and the relationship between security and privacy, data protection, and Payment Card Industry Data Security Standards; identify three categories of challenges and provide recommendations; and discuss the human factor with respect to protecting privacy and monitoring for fraudulent behavior.

Part II, Risks, tackles the relationships of information security risks with others. It contains four chapters.

Part III, Experience, covers a collection of experiences from different sectors. It contains four chapters, each covering one sector: financial services, energy, transportation and academia.

The appendix, Key Information Security Law References, covers US federal and state statutes and regulations, court decisions, and decrees; EU directives; and laws of other countries. This appendix can act as a quick reference.

In its entirety, the book instigates thoughts for future risk and security concerns.

EDITORS’ NOTE
Enterprise Information Security and Privacy is available from the ISACA Bookstore. For information, see the ISACA Bookstore Supplement in this Journal, visit www.isaca.org/bookstore, e-mail bookstore@isaca.org or telephone +1.847.660.5650.
Computer and Information Security Handbook

*Computer and Information Security Handbook* is a very informative handbook for information security professionals, IT auditors, technical specialists, consultants, and students pursuing courses in information technology and computer-security-related fields. It provides a comprehensive presentation of the currently most relevant topics of information security from computer security theory, related technology, practice, security threats/risks, and regulatory and privacy considerations.

It is very valuable for a reader who is looking for a reference book that is a source of factual knowledge and for concise answers to questions that arise when working or doing research in the computer security field.

It is also a great source for IT auditors who want to improve their technical knowledge or practitioners and consultants who are studying for information-security-related certifications. This handbook is a great addition to the information security professional’s technical reference library.

The book features eight parts, 43 chapters with appendices, a glossary of terms common in computer security and an index. All chapters are written by specialists in the field covered by the chapter. To provide a brief view of the scope covered by the book, the eight parts are listed here:

- Overview of System and Network Security: A Comprehensive Introduction
- Managing Information Security
- Encryption Technology
- Privacy and Access Management
- Storage Security
- Physical Security
- Advanced Security
- Appendices

The content is computer security in general and is not limited to a specific industry, system or application. Many examples, charts, tables and figures provide rich support for the presented technical facts and theory. They also provide interesting background information and set the importance of computer security in the right context. Because chapters are independently authored (more than 60 authors), each chapter has its own character in presenting the content and addressing security considerations. Despite that, the overall appearance of the book is homogeneous, as would be expected from a handbook. The structure of the book, sequence of chapters and content presentation is logical and allows, in conjunction with the detailed table of contents and index at the end of the book, an easy navigation through the comprehensive content of about 800 pages.

The strength of the handbook is its broad scope and detailed delivery of knowledge. It is recommended as a reference book for a wide spectrum of readers, from the computer science student up to the information security professional.

**EDITOR'S NOTE**

*Computer and Information Security Handbook* is available from the ISACA Bookstore. For information, see the ISACA Bookstore Supplement in this *Journal*, visit www.isaca.org/bookstore, e-mail bookstore@isaca.org or telephone +1.847.660.5650.
Applying Data Analytics to IS Audit

Efficiency in today’s information systems (IS) audit process is critical to achieve the cost-effectiveness desired in the current economic environment. Applying automated data analytic techniques to audit functions can enable IS audit teams to do more with the same, or fewer, resources. Use of these techniques can assist the IS auditor in complying with ISACA® standards. Effective 1 January 2009, internal auditors, including IS auditors, must (instead of should in the prior standard) “consider the use of computer-assisted technology-based audit tools and other data analysis techniques when conducting internal audits” according to the Institute of Internal Auditors’ (IIA) professional practice standard section 1220.A2.2

Previously, the ISACA Journal has included articles discussing the use of data analytics. This article wishes to expand on the prior articles by providing specific implementations of data analytics to the IS audit scope of the audit universe, moving beyond financial audit techniques. The following sections are an anecdotal collection of IS audit data analytic techniques used by the author and other IS auditors recently.

PLANNING

Many times auditors equate data analytics with fieldwork. While fieldwork may be the most frequent area in which data analytics is deployed by auditors, what is often overlooked is the process of using data analytics as an effective planning tool. When risk-assessing the audit universe to determine the annual audit plan, data analytics may be used to help evaluate risk components that drive the annual deployment of IS audit resources. Most organizations’ IT shops collect, for tracking purposes, incident or help desk tickets across all IT areas. This database of issues, usually rated “high” to “low” in severity, can be loaded into the IS auditor’s data analytics tools and assessed by frequency and severity across multiple departments in the IT organization or across multiple software applications. This evaluation can be combined with other risk factors to help determine the overall IT department risk rating.

Related to efficiency, that same IT incident/help desk ticket database can be reused for planning at the individual engagement level. If, for example, an audit of the systems team is on this year’s plan, the incidents may be grouped by platform (Windows, UNIX, LINUX, etc.) and evaluated for severity and frequency. That evaluation may drive more audit time during the engagement to platforms experiencing the most challenges.

IT organizations’ development efforts, both planned and in process, are usually stored in a project management tool. IS auditors’ analysis of this database can help:

• Drive the IS annual audit plan toward applications development teams experiencing the higher-risk changes
• As an integrated audit tool, inform financial and operational auditors of significant application changes that may affect the timing of a financial or operational audit

FIELDWORK

There is a wealth of examples showing how to apply data analytics to financial transactions. Following are some ideas of how to apply data analytics to IS audit test procedures.

Interpretation of Complex Data

Analysis of Active Directory Groups

To support analysis of access controls over storage repositories (shares) in which sensitive customer or company data are stored, many auditors review user membership in Active Directory (AD) groups for rights appropriate to the user’s job duties. While there are commercial tools to analyze AD, the assumption in this article is that the IS auditor has access to a data analytic tool but not to a commercial AD tool. Built into the AD server is a command that extracts data from AD into a comma-separated values (CSV) file type. The command `csvde -f outputfilename.csv` places the content of all the AD objects (users, computers, groups, etc.) and their settings into a CSV file that loads into most data analysis tools. The groups a user is a member of can then be counted and listed by separating the field “memberOf” based

Michael Hoesing, CISA, ACDA, CDP, CIA, CISSP, CMA, CPA, has more than 30 years of experience in the areas of information systems audit and assurance, information systems implementation, and financial audit. His experiences span a variety of industries during his years with public accounting firms. His last 18 years have focused on financial services with firms such as First Data Corp., First National Nebraska Inc., PricewaterhouseCoopers and American Express. Hoesing has been involved in both the external and internal audit processes and has served as a software trainer.
on the semicolon delimiter, using parsing functions (e.g., SPLIT) built into most data analytic tools, as shown in Figure 1.

Configuration Management
Operating system auditing conquers one of the more typical audit challenges, the lack of data. In fact, operating systems usually provide a wealth of excess data that need to be culled down in order to audit the relevant facts. For example, a VMware ESX 3.5 virtualization host can provide details of the current configuration and operational metrics by issuing the `esxcfg-info` command. Redirecting the output to a text file results in a file of approximately 10,000 records, mostly performance metrics (as shown in Figure 2). Loading the data into an analytics tool requires testing each of the records for an identifier (e.g., level 2 is "\==+" at position 4) using the `TEST` or equivalent function, as shown in Figure 3, then locating descriptions and data within that record.

Once the raw data are read into the analytic tool, filters and searches can be conducted to narrow the data displayed to relevant audit topics. Audit-relevant data for this host can be extracted and saved to a separate file. Repeating this process in the future or with additional hosts could enable building cumulative files to trend the configuration over time to evaluate remediation efforts or for comparison among multiple hosts.

Assessment Tool’s XML Output
Many assessment tools provide data in an Extensible Markup Language (XML) output. While easy to read and navigate, the XML output tends to stack data top to bottom, rather than the more traditional file structure of data flowing from left to right. Also, many free assessment tools provide assessment data for one scan or one host and are not designed to collect data over multiple time periods or for multiple machines. One free tool that

![Figure 1—Active Directory Analysis](image1)

![Figure 2—Configuration and Operational Metrics Output Text File in Notepad](image2)

![Figure 3—Identifying Data Elements With a TEST Function](image3)
may be used to assess Payment Card Industry (PCI) Data Security Standard (DSS) compliance for wireless access points is Kismet.

Kismet’s XML output can be read by most tools that automatically interpret XML metadata and flatten the stacked data as shown in figure 4. Once in an analytic tool, the data can be reviewed for the presence of encryption or other settings, as shown in figure 5.

Adopting techniques from the next section, joining the Kismet results with the known, approved inventory of wireless access points, would help determine unauthorized devices and authorized devices that are dormant. Some may say a dormant device poses little risk; however, should that device be reactivated, the IS auditor may wish to understand the process used to patch and configure a reactivated device to the organization’s current standards, if the requirements have changed during the period of inactivity.

Determining Context Using Multiple Files

Analyzing a single file, even when given unlimited time to do so, may not produce useful audit information. Many times additional data in secondary files are needed to fully understand and give context to the original file. Examples applicable to IS audit include:

- **Logical access**—Combining a logical access file with an HR employment file will help determine which user accounts are aligned with valid employees. Also, if the access functionality of the user’s profile can be combined with the initial two files, comparison of a user’s work department with the capabilities granted to him/her can be evaluated for appropriate segregation of duties.
**Change control**—File library listings can be combined with data from the change management system and dates of file changes can be matched to dates of authorized events in the change management database to help identify any unauthorized changes.

**Physical security**—Matching of ingress records to egress records could be performed to help identify tailgated access to sensitive IT areas. If both records are in one file, analytic tools may be used to reorganize the data by badge number and by date/time stamp using sorting tools, and then the current record can be compared to the previous record with a RECOFFSET function to determine if egress succeeded an ingress record.

**REPORTING**

Analytic tools have extensive capabilities to group and summarize data, bringing perspective to the analysis. The list of devices found in the scan results shown in figure 5 could be combined with an organization’s actual inventory of authorized devices. Reports could then be derived showing unauthorized devices, or authorized devices that were not on and active and were not discovered by the scan. The former contains the risk of unauthorized and possibly incorrectly configured devices, and the latter has the risk that dormant authorized devices are not enabled and are not receiving current patches. This detail will help IS management or the audit committee to understand the magnitude of the rogue device and configuration problems and the effort needed for correction.

Also, with the event tickets system noted previously, IT management, which, like IT audit, has too much to do in too little time, may be focused on solving the current high risk-rated events. This leaves little time for analysis. If the auditor can provide additional insights to the event data (volume by platform, volume by application, volume by time period), management may be able to address some recurring topics and reduce the event rate.

Summarization and grouping of data may also be used by the auditor when reporting to the audit committee. Showing the committee that the auditor wishes to place platform X on next year’s schedule, instead of platform Y, due to the number of critical applications supported, the number of significant event tickets issued and IT staff hours devoted to support, based on verifiable metrics, may be better received by the committee (and the chief information officer), than more subjective measurements.

**CONCLUSION**

The ideas presented here can be expanded almost infinitely based upon the environment and needs of the auditor’s organization, and are limited only by one’s imagination. IS auditors can continue to fulfill the data analytic support role to financial or operational audits, but should also apply those skills to completing their own portion of the audit plan.

**ENDNOTES**

1. ISACA IT Audit and Assurance Standards that help to explain where to use data analytics include: S5 Planning, S6 Performance of Audit Work, S11 Use of Risk Assessment in Audit Planning, S12 Audit Materiality, S14 Audit Evidence, www.isaca.org/standards. Also, IT Audit and Assurance Guideline G3 Use of Computer-assisted Audit Techniques (CAATs) provides guidance on how to use data analytics in IS audits.

2. Institute of Internal Auditors, International Standards for the Professional Practice of Internal Auditing (Standards), www.theiia.org


5. During the course of the past couple of years, the author has had the opportunity as a software trainer and educator to discuss IS audit techniques, data analytic techniques and other techniques with a variety of IS audit professionals across the country. While it would be impossible to match names with each technique presented here, the author would like to extend a collective “thank you” to all whose path he has crossed and who have provided him with their thoughts.

6. Baker, Neil; “Software Trend Spotting,” Internal Auditor, August 2009. While not all-inclusive, according to the IIA survey, top data analysis tools include ACL, Microsoft Excel, Microsoft Access and IDEA.

7. While not all-inclusive, a Google search produces commercial tools such as Hyena, GFI lanGard and ScriptLogic.


Synthesizing SAS 70 Audits and PMI’s Project Management Process Groups
Using Project Management Principles to Optimize the SAS 70 Auditing Process

All projects at some point will come under fire, and in an uncertain economy, increased pressures to derive optimal value emphasize the need to deliver project success. Statement on Auditing Standards No. 70 (SAS 70), Service Organizations, audits can be expensive, particularly Type II audits. As companies are reducing budgets and staff, justifying the cost of this audit becomes important, with value and expectations increasing. Companies with smaller staffs and/or increased reliance on outsourcing are realizing that strong process is the key to better application development and avoiding expensive rework. Even in accelerated SAS 70 Type I project life cycles, project management (PM) best practices can be exercised.

Process is not about reinventing the wheel; rather, it is finding what has worked in the past and applying it to the present, using strong communication to deliver and manage these processes and paring away anything that diverts the team from project goals. The ultimate challenge for project management is to find a repeatable process and communicate it clearly so that multiple levels within an organization accept and support the benefits. The key to best practices in project management is no mystery; it lies in the execution.

PM is a process by which projects are defined, planned, organized, monitored, controlled and delivered in such a way that the agreed-upon goals are realized given the project’s scope, schedule, cost and quality constraints. Projects are unique, temporary undertakings with a start date and an end date (or end condition).

SAS 70, which provides for a uniform approach to reporting, is a defined standard developed by the American Institute of Certified Public Accountants (AICPA) as a set of criteria a service or user organization’s auditor should use while assessing the outsourced internal controls of a service organization. Service organizations typically provide outsourcing services that may affect the operations of the contracting company or user organization; such services may include transaction processing, web hosting, hosted data centers, paper shredding, credit processing, etc.

AICPA defines a standard for uniform audit reporting of SAS 70 audit findings without regard to the process of conducting an audit. A SAS 70 audit engagement is effectively a project with all the characteristics described in the Project Management Body of Knowledge (PMBOK) and could conceivably benefit from applying the best practices, tools and techniques of project management.

SAS 70 audit projects are distinctive and temporary, requiring a progressively elaborate set of auditing tasks that lasts for a couple of days to several months based on the type of audit. Regardless of the type of audit, the end result is a SAS 70 audit report commissioned at the request of the project sponsor (which is either a service organization or user organization). These audits are performed by accounting firms, often in collaboration with a Certified Information Systems Auditor™ (CISA®) along with other IT specialists as needed based on the scope of the audit.

This article will explore how a SAS 70 audit is improved by understanding and applying PM tools and techniques. To this end, the basic tenets of PM principles, as defined in A Guide to the Project Management Body of Knowledge (PMBOK Guide), will be examined and synthesized with the SAS 70 auditing process, emphasizing the ways to optimize SAS 70 auditing performance.

Thomas J. Bell III, Ph.D., CISA, is a professor of business administration in the School of Business at Texas Wesleyan University in Fort Worth, Texas, USA, and an IT security auditor for ComputerMinds.com in Euless, Texas, USA. His IT auditing specialty is IT audits for small community banks (IT security audits and external penetration testing) and SAS 70 Type I and II audits.
WHAT IS A SAS 70 AUDIT?

SAS 70 is an auditing statement developed by the Auditing Standards Board of the AICPA. A SAS 70 audit is broadly recognized because it provides reasonable assurance that a service organization has been through an in-depth audit of its control activities, which generally include controls over IT and related processes.

In cases where data are regulated and/or sensitive, it is important for service organizations to have detailed and well-documented controls in place to ensure the safety and privacy of the data being processed, stored and transmitted. Perhaps most notably, the requirements of section 404 of the US Sarbanes-Oxley Act of 2002 heighten the importance of SAS 70 audit reporting on the effectiveness of internal control over financial reporting. A SAS 70 audit serves as an indicator of transparency and accountability; it establishes a high level of commitment by the service organization toward ensuring the reliability and security of its data by having its internal controls and activities examined (via an in-depth audit of control) by an independent auditing firm.

SAS 70 provides guidance to service auditors when they assess the internal controls of a service organization and issue a service auditor’s report. SAS 70 also provides guidance to auditors of financial statements of an entity that uses one or more service organizations. Service organizations are typically entities that provide outsourcing services that impact the control environment of their customers or user organization. Examples of service organizations are insurance and medical claims processors, trust companies, hosted data centers, application service providers, managed security providers, credit processing organizations, and clearinghouses, to name a few.

A formal report, called a service auditor’s report, which includes the auditor’s opinion or attestation statement, is issued to the service organization at the conclusion of a SAS 70 audit. This report is effectively an auditor-to-auditor communication between the service organization and user organization (the entity that has engaged a service organization, particularly if its financial statements are impacted by the services of the service organization).

TYPES OF SAS 70 AUDITS

There are two different, yet complementary, types of SAS 70 audit reports, a Type I or Type II audit. Type I includes an opinion of the fairness of the presentation of the service organization’s description of controls that had been placed in operation and the suitability of the design of the controls to achieve the specified objectives. Type I reports describe the degree to which the service organization fairly represents its services in regard to controls that have been implemented in operations and its inherent design to achieve objectives set forth. This report typically examines controls only over one or two days, which arguably has limited value to a user organization.

A Type II service auditor’s report is the more thorough report of a SAS 70 audit because it contains a description of the controls in place and a description of the auditor’s tests of control effectiveness for a minimum testing period (usually the defined period is six months, but it can be longer). The Type II examination of the SAS 70 audit process begins the same as Type I, but adds more testing and observing procedures. These procedures analyze and test the controls vis-à-vis the Type I, which merely describes the controls in place. The Type II service auditor’s report states “whether the controls that were tested were operating with sufficient effectiveness to provide reasonable, but not absolute, assurance that the control objectives were achieved during the period specified.”

A Type II service auditor’s report is more common and often the preferred choice of SAS 70 audits because it is a comprehensive analysis of not only what controls are in place, but how effective those controls are in meeting the desired objectives.

WHAT IS PM?

The PMBOK Guide is a collection of processes, process groups and knowledge areas generally accepted as best practice within the PM discipline. As an internationally recognized standard (IEEE Std 1490-2003), it provides the fundamentals of project management, irrespective of the type of project.

The PMBOK Guide defines PM as “the application of knowledge, skills, tools and techniques to project activities to meet project requirements.” In many ways, PM is a framework or guide for achieving goals while optimizing the use of resources (e.g., people, time, capital).

PM is, ultimately, about applying the appropriate skills to attract and manage the right team while using tools and techniques to get the job done to specification, on time and within budget. One of the traditional ways to measure
whether a project’s objectives are being met is through Triple Constraint. PM Triple Constraint has been defined a number of ways. For this article, the variation of definitions is negligible since the challenge of every project is to be successful within the Triple Constraint framework. Triple Constraint consists of scope (project size, goals, requirements), cost (people, equipment, material) and schedule (task durations, dependencies, critical path), with quality (meeting or exceeding customer or sponsor satisfaction) serving as the requisite criterion for the three constraints. The three elements of a project are known to work in tandem with one another, forming an equilateral triangle that remains equilateral as elements are adjusted over time. Where one of these elements is restricted or extended, the other two elements will then also need to be either extended/increased in some way or restricted/reduced in some way.

Triple Constraint involves making trade-offs among scope, time and cost for a project. It is inevitable in a project life cycle that there will be changes to the scope, time or cost. Where many projects encounter difficulty is when one of the areas changes and appropriate adjustments are not made to the other areas. There is an ongoing balancing of the three elements that requires a skillful project manager who understands planning, resourcing and executing/controlling a project. The project manager is accountable for accomplishing the stated project objectives, oversees all the work identified to complete the project, and applies various tools and techniques. A project manager must simultaneously manage the four basic elements of a project: quality, cost, schedule and scope.

**SAS 70 AUDITING AND PM PRINCIPLES**

Before synthesizing SAS 70 audits with PMBOK principles, it is important to demonstrate the parallel relationship between SAS 70 audits and PM principles. The association between the SAS 70 audit process and the concept of a project is outlined in figure 1.

All projects should have a well-defined objective or goal; a SAS 70 audit goal is either a Type I or a Type II audit report. A project should have a primary sponsor, who is the person responsible for providing direction and funding for the project; the SAS 70 audit sponsor is usually a senior manager or member of upper management. Another project characteristic is its uniqueness and sequencing of activities. Each SAS 70 audit must be uniquely tailored to the organization’s transaction processing controls, with appropriate sequencing of incremental audit tasks. SAS 70 audits should have a specified start and finish time frame, along with some allocated resources that comply with the attributes of the audit.

Since SAS 70 audits ostensibly meet all the attributes of a project as defined by PMBOK, it stands to reason that understanding and applying the best practices of PM are also beneficial to the SAS 70 process. Refer to figure 1 for a detailed listing of the SAS 70 audit project.

**SYNTHESIZING SAS 70 AUDITS WITH PM TECHNIQUES**

Managing a SAS 70 project, as with any project, consists of executing defined activities to achieve project objectives. These project activities or processes, as defined by PMBOK, are quite similar for most projects. PM processes are grouped into five different process categories—each process constitutes a series of tasks directed toward some result. The process groups are initiating, planning, executing, monitoring and controlling, and closing. The process groups are linked by the output they produce; that is to say, inputs serve as the prerequisites or entry criteria to start the next process. Outputs are the exit criteria or the result of the process with which the process ends; the output of one process generally becomes an input to another process.

Performing a SAS 70 audit is a structured, multistep process that includes a number of predefined processes and procedures that must take place to ensure its successful and timely completion. Depending on the needs of the requesting organization, a SAS 70 Type II audit is generally performed for a specified period following the completion of a Type I. Generally, successfully completing a SAS 70 Type I and then moving toward Type II compliance for subsequent years is the most common path many service organizations choose.5

SAS 70 Type I and Type II audits are potentially improved by using the best practices of PM as identified in the PMBOK Guide process groups. Each PM process within the process groups is correlated to the SAS 70 audit process, as shown in figure 2.

**INITIATING PROCESS AND SAS 70 AUDIT**

The SAS 70 initiation process is launched after soliciting or responding to a request for proposal (RFP) with a contract that commonly includes the cost of work; background and experience of the auditors; audit methodology; deliverables;
A preliminary review, also referred to as a readiness review, is often performed for service organizations that are new to the SAS 70 audit process. The purpose of a readiness review is to define the key control objectives and control activities that will be covered in the forthcoming SAS 70 audit(s) and to identify those control weaknesses that need to be corrected prior to the SAS 70 Type I or Type II audit engagement.

When defining the scope, ideally the user organizations will have significant input into the scope or systems to be covered by the service organization’s SAS 70 audit. In practice, the service organization largely determines the audit scope based on its relationship with the user organizations or selective audit objectives deemed important.

Establishing a scope statement should follow a structured initiation process beginning with an audit contract that establishes executive understanding and commitment before...
<table>
<thead>
<tr>
<th>PM Process Group</th>
<th>SAS 70 Audit Process</th>
<th>PMBOK Process Description</th>
</tr>
</thead>
</table>
| **Initiating**   | • Establish engagement terms.  
                 | • Complete preliminary review.  
                 | • Establish materiality and assess risks.  | Defines and authorizes the project or a project phase by management  
| SAS 70 initiating processes: | | Input: Usually a statement of work or a contract, policies, procedures and organizational culture  
| • Initial discussion occurs between the service auditor and service organization for the purposes of understanding the scope, timing and final deliverables of the audit. | | Output: Project charter and a preliminary project scope statement  
| • The service organization undergoes a service auditor SAS 70 readiness assessment. | |  
| • The service auditor reviews, analyzes, and makes comments and recommendations regarding the information obtained during the SAS 70 readiness assessment. | |  
| • The service auditor and service organization collectively agree on any areas within the service organization’s control environment that require remediation prior to beginning the SAS 70 Type I or Type II fieldwork. | |  
| • The service auditor sends to the client a list that consists of documents and other deliverables that must be prepared prior to commencement of the SAS 70 Type I or Type II fieldwork. | |  
| **Planning**    | • Plan the audit.  
                 | • Understand the internal controls. | Defines and refines objectives, and plans the course of action required to attain the objective and scope  
| SAS 70 planning processes: | | Input: Project charter and a preliminary project scope statement  
| • Meet with the team, stakeholders and sponsors to discuss the objective, risks and benefits. | | Output: PM plan (A PM plan, as defined by the PMBOK Guide, is a comprehensive document that usually defines how the audit project is to be executed, monitored and controlled. It may take on a summary or detailed form that is comprised of one or more ancillary management plans and other planning documents—typically including areas such as audit scope, control objectives and related control activities.)  
| • Determine the schedule, activities, durations, milestones, due dates, resources, cost and budget. | | The objective of a PM plan is to define the approach to be used by the audit team to deliver the intended audit scope of the project.  
| • Assess requirements. | | The project manager facilitates the creation of the PM plan by soliciting input from the service organization, audit team and key stakeholders. The plan should be agreed upon and approved by at least the audit team and its key stakeholders.  
| • Identify risk mitigation techniques. | |  
| • Publicize the plan. | |  
| • Delegate and empower project or team leaders to manage tasks within their areas of expertise, and work closely to keep communication open. | |  
| • Keep everyone on task by meeting regularly. | |  
| **Executing**   | • Perform audit procedures.  
                 | • Test controls.  
                 | • Complete audit sampling. | People and other resources combined with the PM plan to carry out, or execute, the plan for the project  
| SAS 70 executing processes: | | Input: PM plan  
| • Team members actively communicate via regular information sessions. | | Output: Project deliverables, such as meetings (scope, readiness, audit findings review), fieldwork, testing controls (if appropriate) and draft/final SAS 70 Service Auditor’s Report  
| • Develop standard criteria for measurement, such as meeting deliverables, defect detection, resource utilization and rework. | |  
| • Use software configuration management or requirements management tools to automate and manage the change process. | |  
| • Establish a chain of command for approving any scope change for the project. | |  

starting a project. The project manager should ensure that a project has a designated project sponsor and should gather the necessary business and technological criteria to justify the project continuing with adequate executive support during its life cycle.

PM tools and techniques support the initiation processes—establishing the nature and scope of the project. Best practices for this stage suggest that if it is not performed well, it is unlikely that the project will be successful in meeting the business’s needs. The key project controls needed here are understanding the business environment and ensuring that all necessary controls are incorporated into the SAS 70 project.

**Planning Process and SAS 70 Audit**

After the initiation stage, the project is planned to an appropriate level of detail. The central purpose is to plan the work in terms of time, cost, people and other resources and in such a way that work estimates are possible and probable risk is identified. As with the initiation process group, failure to plan sufficiently significantly reduces the project’s chances of successfully conducting a SAS 70 audit.

Project planning generally consists of producing a project plan that includes the following:

- Determining the audit category (Type I or Type II)
- Further refining the scope statement
- Creating a work breakdown structure (WBS) and identifying deliverables
- Defining activities, durations and logical sequencing
- Estimating the resource requirements for the activities
- Estimating time and cost for activities
- Planning quality
- Developing a human resource plan
- Developing the schedule
- Developing the budget
- Identifying risk and planning risk management

Comprehensive planning is critical, even with short development cycles for Type I audits. Project goals should be made attainable by prioritizing deliverables to keep a team tightly focused on specific issues. To understand exposures and the dangers to the project, the team, stakeholders and sponsors should be routinely involved in closely managed sessions to
discuss each objective and clearly explain risks and benefits.

SAS 70 project planning is perhaps the most difficult and unappreciated process in the project stages. The central purpose of SAS 70 audit project planning is to guide audit execution. And, to guide execution, plans must be realistic and useful; this often requires an inordinate amount of time and effort. Best practices suggest audit planning should be a team effort with task-knowledgeable people planning the work. A basic planning tenet is: “A dollar spent up front in planning is worth one hundred dollars spent after the system is implemented.”

EXECUTING PROCESS AND SAS 70 AUDIT
Executing a SAS 70 audit involves coordinating people and resources, as well as integrating and performing the activities of the audit in accordance with the project management plan. Successfully executing a SAS 70 Type I or Type II audit involves developing the audit team to perform, according to the PM plan, information distribution and contract administration.

The project manager for the SAS 70 audit engagement is responsible for accomplishing the PM plan by integrating the following audit activities into one coordinated effort. These activities broadly include:

- Coordinating an initial meeting to understand the scope, timing and final deliverables of the audit
- Requesting the service organization to submit its SAS 70 readiness assessment for review, if available. Otherwise, a readiness assessment should be performed.
- Facilitating a meeting for SAS 70 auditors and the service organization to collectively agree on any areas within the service organization’s control environment that require remediation prior to beginning the SAS 70 Type I or Type II fieldwork
- Listing the documents and other deliverables that must be prepared prior to commencement of the SAS 70 Type I or Type II fieldwork
- Directing the SAS 70 auditing team fieldwork activities based on the type of SAS 70 audit. Fieldwork may include the following:
  - Performing tests to evaluate appropriateness and operating effectiveness of control design (Type II only)
  - Identifying and communicating control deficiencies to management
  - Recommending required controls and guidelines to management
  - Facilitating the preparation of an initial draft report and coordinating meetings with the service organization to discuss findings
  - Coordinating the final closing meeting between the service auditors and the service organization to discuss the final SAS 70 service auditor’s report and management’s comments
  - Issuing the final SAS 70 service auditor’s report

Effective audit execution makes use of all the stakeholders (sponsor, clients, project team, support staff and so on) involved in the project. People are the single most important asset in organizations and on audit projects. As such, people perform much more effectively if they are in active communication with each other so that each dependency is clearly understood and managed. Holding weekly information sessions with the team to discuss issues and to collectively figure out correction strategies is yet another principle gleaned from PM best practices. If the team is scattered, the project manager should use collaborative tools to hold meetings and share information. The method is not as important as the ongoing communication activity itself.

MONITORING/CONTROLLING PROCESS AND SAS 70 AUDIT
Monitoring and controlling consists of those processes performed to observe project execution so that potential problems can be identified in a timely manner and corrective action can be taken, when necessary, to control the execution of the audit project. The key benefit is that audit performance is observed and measured regularly to identify variances from the PM plan.

Monitoring and controlling includes:

- Measuring the ongoing audit activities
- Monitoring the project variables (cost, effort, scope, etc.) against the PM plan and the audit performance baseline
- Identifying corrective actions to address issues and risks properly
- Influencing the factors that could circumvent integrated change control so only approved changes are implemented

To assess the status of the audit, the project manager should schedule meetings regularly. Issues discussed during these meetings may include actual progress vs. work and cost estimates, requirements measurement for scope control, and overall quality measurements in productivity. The actual process is very flexible. Using the audit project charter as a guide, the team should prepare criteria that measure the entire project,
and then use subsets of those criteria for assessment with each milestone. Short life cycle projects, i.e., Type I audits, can also benefit from regular meetings as long as they ensure that time is not wasted. Meetings should be kept short and to the point. Standard criteria for measurement, such as meeting deliverables, defect detection, resource utilization and rework, should be developed to find out where improvements are needed.

CLOSING PROCESS AND SAS 70 AUDIT
Closing includes the formal acceptance of the audit report and usually a debriefing meeting. Administrative activities include the archiving of the files and documenting lessons learned. This phase consists of:
• Finalizing all activities across all of the process groups to formally close the project or a project phase
• Completing and settling the contract (including the resolution of any open items) and closing each contract applicable to the project or project phase
• Issuing the SAS 70 audit report

A postmortem audit review should be conducted. This is the time to hash out any issues that will improve audit support and improve process for the next audit project. All audit issues that caused any delays or restructuring of project focus, implementation issues and support problems should be collected and noted.

CONCLUSION
SAS 70 audits have grown increasingly popular with the implementation of the Sarbanes-Oxley Act and its mandate for demonstrating the effectiveness of a service organization’s internal controls and data security safeguards. The primary challenge of SAS 70 audits as they relate to PM is to achieve all of the project goals and objectives while managing the ever-present scope, schedule and budget constraints that, according to the Standish Group, have thwarted many projects.

SAS 70 Type I or Type II audits are arguably an organizational investment since considerable time, money and other resources are committed with an expectation of receiving something of value in return. And, since SAS 70 audits are in fact projects (by virtue of meeting the criteria of a project as shown in figure 1), they stand to benefit from the best practices of PM as outlined in the PMBOK Guide.

The PMBOK Guide offers a framework that facilitates combining the body of knowledge of project management along with the body of knowledge of SAS 70 auditing, which allows for an improved philosophy and method for planning and managing a SAS 70 audit. The aggregate of SAS 70 auditing and project management bodies of knowledge provides a foundation for a logical, repeatable approach that improves the likelihood of successfully delivering value to the organization via a SAS 70 audit.

Aggregating SAS 70 auditing and PM bodies of knowledge can be overwhelming at first glance; however, a more prudent approach for audit projects would be to tailor the PMBOK Guide according to the project, rather than exhaustively attempting to address all the process areas. A tailored approach is best supported by creating and regularly updating a best practice library of methods that have worked for previous projects. This library should be a living repository that grows with each completed audit project. As audits are completed, a postmortem review should be performed to update or change procedures for continual improvement. The general rule of thumb is to strive for modularity, so that processes and procedures can be customized for a specific project based on size, complexity, team structure, etc.

ENDNOTES
4 Ibid.
6 Author unknown
7 Johnson, Jim; “CHAOS: The Dollar Drain of IT Project Failures,” Application Development Trends, January 1995
Would one buy a house when the stability of the foundation is uncertain? Would one make a payment if the accuracy of the bill is in question? If the answer is no, then why would any organization settle for making business decisions based on inaccurate and inconsistent data warehouse information? A number of studies show that much of the data warehouse information available to business users is not accurate, complete or timely. Despite significant investment in data warehouse technologies and efforts to ensure quality, the trustworthiness of data warehouse information at best remains questionable. Current approaches to restore trust in data warehouse information are often heroic efforts of the individuals responsible for the data warehouse and include:

- Manual or semiautomated balancing, tracking and reconciliation to prove accuracy
- Ad hoc queries of data sources to support "audit needs"
- Extensive research and remediation to identify, diagnose and correct issues

These approaches provide short-term respite but are not sustainable in the long run. The increased labor cost for manual processes and the high processing cost for reruns when errors are identified late in the process increase ongoing operational costs. The cumbersome and costly processes for supporting audit needs also create organizational stress. Frequently, a large number of data warehouse projects are abandoned because of the high costs of efforts to ensure information quality.

While standardized tools, such as those for extraction, transformation and loading (ETL) and data quality processes, solve part of the problem, there is an urgent need for adopting a systematic approach for establishing trust in data warehouse information. The proposed approach outlines a framework for ensuring the integrity of data warehouse information by using end-to-end information controls.

ROOT CAUSES OF INFORMATION QUALITY ISSUES

While several factors can be attributed to the information quality issues, the following are the major causes of information errors within data warehouses:

- Changes in the source systems—Changes in the source systems often require code changes in the ETL process. For example, the ETL process corresponding to the credit risk data warehouse in a particular financial institution has approximately 25 releases each quarter. Even with appropriate quality assurance processes, there is always room for error. The following list outlines the types of potential errors that can occur because of changes in the ETL processes:
  - Extraction logic excludes certain types of data that were not tested.
  - Transformation logic may aggregate two different types of data (e.g., car loan and boat loan) into a single category (e.g., car loan). In some cases, transformation logic may exclude certain types of data, resulting in incomplete records in the data warehouse.
  - Similar issues are also observed with the loading process.

- Process failures—Current processes may fail due to system errors or transformation errors, resulting in incomplete data loading. System errors may include abends due to the unavailability of source system/extract or the incorrect format of the source information. Transformation errors may result from incorrect formats.

- Changes/updates in the reference data—Outdated, incomplete or incorrect reference data will lead to errors in the data warehouse information. For example, errors in the sales commission rate table may result in erroneous calculation of the commission amount.

- Data quality issues with the source system—The source system’s data may be incomplete or...
inconsistent. For example, a customer record in the source system may have a missing zip code. A similar source system related to sales may use an abbreviation of the product names in its database. Incompleteness and inconsistency in source system data will lead to quality issues in the data warehouse.

**CURRENT APPROACH AND COST OF QUALITY**

The current focus in most data warehouse initiatives is to use ETL tools to standardize the data transfer process and to use data quality solutions to detect and correct incomplete and inconsistent data. While these efforts result in significant improvements, data warehouse teams rely on a number of manual/semi-automated processes to balance and reconcile the data warehouse information with the source system information. Some of the techniques currently used by various organizations are:

- Developing an independent script that compares the record count and amount information from the source system with the record count and amount information from the data warehouse. These scripts are often executed either on an ad hoc basis or scheduled to run after the data load is complete.
- Creating a control table and then populating the control table with the totals from the data warehouse and the source system as part of the ETL process. Checks are performed after the completion of the load process.

While these methods are somewhat effective in detecting the errors, they rely heavily on the ETL process, which is often the source of the error. More important, these approaches are not effective when the transactions from source systems are either split into several transactions or combined into a single transaction. Such scenarios require advanced logic for balancing the information between the source system and data warehouse. In addition, the inability to reconcile detail-level information using scripts or ETL processes does not allow users to pinpoint the exact issue, resulting in significant manual research and resolution efforts. In addition to the high operational costs related to research and reruns to ensure quality, the current approach impacts the morale of the data warehouse team and the confidence of the business users.

The problem of data quality exacerbates when the data warehouse information is used for storing and reporting financial information. In this scenario, internal audit requests evidence of controls’ operation and documentation related to error resolutions when controls detect errors. Such requests are often met by querying a myriad number of log files, e-mail chains and data warehouse tables. This increases the workload of the data warehouse resources and increases the rift between audit and data warehouse teams.

Current approaches are not scalable and sustainable. There is an urgent need to use automated information controls for verifying, balancing, reconciling and tracking the data warehouse information. Ideally, information controls should be independent of the underlying application and should have the ability to store an audit trail of the information transfer process and its validation results.

**THREE PILLARS FOR ENSURING DATA WAREHOUSE QUALITY**

Successful and cost-effective data warehouse quality initiatives in Fortune 500 organizations are founded on three critical pillars, as shown in figure 1.

*Data quality (DQ) tools*—Identify, correct and standardize incomplete and inconsistent source system information prior to loading to data warehouses. The focus of these solutions primarily has been on validating customer addresses and product names. These solutions often do not address the quality issues of the financial transactions.

*ETL tools*—Extract and transform source system information and load it into the data warehouse. The primary focus has been standardizing and increasing the efficiency of the data transfer process.
• **Information control (IC) solutions**—Verify, balance, reconcile and track information as the source system data traverse through various points in the ETL process to the data warehouse. The focus has been to independently ensure the accuracy, consistency and completeness of the information at both an aggregate and transaction level.

Information controls not only balance and reconcile the data before and after the load, but also can be expanded outside the scope of the data warehouse to ensure that the data warehouse information is aligned with other critical applications such as the general ledger (GL). For example, although the same journal systems may feed both the data warehouse and the GL, manual adjustments in the GL system may cause an out-of-sync condition that could be detected early if an automated information control is in place. In addition, automated information controls store the audit trail information about the control actions and the resolutions in case of exceptions. Figure 2 compares ETL and DQ tools with IC solutions from various aspects.

### INFORMATION CONTROLS FRAMEWORK FOR DATA WAREHOUSE

The proposed framework recommends a minimum of six information controls to achieve the objectives of the data warehouse quality initiatives. The locations of the information controls are depicted in Figure 3. The six controls are:

1. **Control X1, data warehouse to source system validation**—Ensure that the data warehouse information can be balanced and reconciled with the source system. In addition to validating the number of records, controls should balance the total amount and the amounts at the record key level. The control should also be able to verify that the data being loaded to the data warehouse are not duplicates and are within the set thresholds (i.e., a source file on average contains 1,000 records and has a total amount of US $2.5 million with a tolerance of +/- 10 percent). A notification should be sent if the tolerance is violated.

2. **Control X2, verification between feeds that the data are accurate and complete**—Ensure that the related source feed information is consistent. For example, if one feed consists of credit card payment information and another feed consists of account credit information based on payment information, there needs to be a control to validate the consistency between these two feeds (i.e., validate that the payment information can be reconciled with the credit information).

3. **Control X3, validation that the ETL process is accurate and complete**—The control should monitor transactions and processes, e.g., source to ETL, data warehouse to data mart. Validate adherence to all process dependencies. Automated independent controls could also be used to automate ETL testing.

4. **Control X4, verification within the data warehouse that information is consistent**—Many data warehouses do not enforce referential integrity. Changes in the data update process by downstream applications can result in data discrepancies. Independent controls should be used to ensure referential integrity is maintained by reconciling relevant information.

<table>
<thead>
<tr>
<th>Control X1, data warehouse to source system validation</th>
<th>Provide an efficient means to profile and clean data warehouse information either before loading or after loading.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Control X2, verification between feeds that the data are accurate and complete</td>
<td>Provide an efficient means to extract, transform and load information to the source system.</td>
</tr>
<tr>
<td>Control X3, validation that the ETL process is accurate and complete</td>
<td>Read data from a number of sources.</td>
</tr>
<tr>
<td>Control X4, verification within the data warehouse that information is consistent</td>
<td>Provide end-to-end independent control to:</td>
</tr>
<tr>
<td></td>
<td>• Verify information</td>
</tr>
<tr>
<td></td>
<td>• Balance information</td>
</tr>
<tr>
<td></td>
<td>• Reconcile information</td>
</tr>
<tr>
<td></td>
<td>• Track information</td>
</tr>
</tbody>
</table>

**Figure 2—ETL Tools, DQ Tools and IC Solutions Comparison**

<table>
<thead>
<tr>
<th>Data Quality Tools</th>
<th>ETL Tools</th>
<th>Information Control Solutions</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Primary use</strong></td>
<td>Provide an efficient means to profile and clean data warehouse information either before loading or after loading.</td>
<td>Provide an efficient means to extract, transform and load information to the source system.</td>
</tr>
<tr>
<td><strong>Benefits</strong></td>
<td>Work with a number of data types. Mostly work with one data source at a time. Extensively use master data lists. Detect and clean data errors as they relate to name, addresses and product names.</td>
<td>Extract data from many sources and many formats. Include a wide range of transformation capabilities. Efficiently load data to a number of databases.</td>
</tr>
<tr>
<td><strong>Audit support</strong></td>
<td>Point-in-time audit trail</td>
<td>Limited audit trail</td>
</tr>
<tr>
<td><strong>Visibility support</strong></td>
<td>Provide visibility to IT.</td>
<td>Provide visibility to IT.</td>
</tr>
</tbody>
</table>
5. **Control X5**, assurance that the data balance with downstream applications or data marts—Ensure that the data warehouse information can be balanced and reconciled with the downstream processes.

6. **Control X6**, validation between parallel systems and the data warehouse—Data warehouse information can also reside in other systems. For example, loan information resides both in the GL and the credit risk data warehouse. It is important to reconcile the information in the parallel system with the data warehouse information. In the absence of such a control, the loan information in the financial reports, generated from the GL system, may become out of sync with the loan information used for estimating the capital requirements for Basel II.

**CONCLUSION**

With the accelerating changes in the source systems to support business needs, increasing reliance on data warehouse information for critical business operation and decisions, and an expanding (and ever-changing) array of regulations and compliance requirements, the use of automated information controls is no longer an option; it is the only way to ensure information accuracy within the data warehouse and across the enterprise. Successful organizations expand the scope of information controls beyond the scope of the data warehouse by developing a companywide program for ensuring the enterprise information quality. With an appropriate selection of tools and frameworks for information controls, organizations can achieve the elusive goal of having higher-quality enterprise information assets.

**ENDNOTES**

1. English, Larry; *Improving Data Warehouse and Business Information Quality*, Wiley and Sons, USA, 2000
2. Eckerson, Wayne W.; *Data Quality and the Bottom Line*, TDWI research series, USA, 2001
3. Friedman, Ted; *Data Quality “Firewall” Enhances Value of the Data Warehouse*, Gartner Report, USA, 2004
Prepare for the 2010 CISA Exams

ORDER NOW—
2010 CISA Review Materials for Exam Preparation and Professional Development

To pass the Certified Information Systems Auditor™ (CISA®) exam, candidates should have an organized plan of study. To assist individuals with the development of a successful study plan, ISACA® offers several study aids and review courses to exam candidates.

www.isaca.org/elearning
www.isaca.org/cisareview

To order CISA review material for the December 2010 exam, visit the ISACA web site at www.isaca.org/cisabooks or see pages S1-S8 in this Journal.

CISA Review Manual 2010
ISACA

The CISA® Review Manual 2010 is a comprehensive reference guide designed to assist individuals in preparing for the CISA exam and individuals who wish to understand the roles and responsibilities of an information systems auditor. The manual has evolved over the past editions and now represents the most current, comprehensive, globally peer-reviewed information systems auditing management resource available.

The CISA Review Manual 2010 features a new format. Each of the six chapters has been divided into two sections for focused study. The first section of each chapter contains the definitions and objectives for the six areas, with the corresponding tasks performed by information systems (IS) auditors and knowledge statements (required to plan, manage, and perform IS audits) that are tested on the exam.

Section 1 is an overview that provides:
• Definitions for the six areas
• Objectives for each area
• Descriptions of the tasks
• A map of the relationship between each task to the knowledge statements
• A reference guide for the knowledge statements, including the relevant concepts and explanations
• References to specific content in section 2 for each knowledge statement
• Sample practice questions and explanations of the answers
• Suggested resources for further study

Section 2 consists of reference material and content that supports the knowledge statements. Material included is pertinent for CISA candidates’ knowledge and/or understanding when preparing for the CISA certification exam. In addition, the CISA Review Manual 2010 includes brief chapter summaries focused on the main topics and case studies to assist candidates in understanding current practices. Also included are definitions of terms most commonly found on the exam.

This manual can be used as a stand-alone document for individual study or as a guide or reference for study groups and chapters conducting local review courses.

The 2010 edition has been developed and is organized to assist candidates in understanding essential concepts and studying the following job practice areas:
• IS audit process
• IT governance
• Systems and infrastructure life cycle management

• IT service delivery and support
• Protection of information assets
• Business continuity and disaster recovery

CRM-10 English Edition
CRM-10F French Edition
CRM-10I Italian Edition
CRM-10J Japanese Edition
CRM-10S Spanish Edition

CISA Review Questions, Answers & Explanations Manual 2010
ISACA

The CISA® Review Questions, Answers & Explanations Manual 2010 consists of 800 multiple-choice study questions that have previously appeared in the CISA® Review Questions, Answers & Explanations Manual 2008 and the 2008 and 2009 supplements. Many questions have been revised or completely rewritten to recognize a change in job practice, be more representative of the current CISA exam question format, and/or provide further clarity or explanation of the correct answer. These questions are not actual exam items, but are intended to provide CISA candidates with an understanding of the type and structure of questions and content that have previously appeared on the exam. This publication is ideal to use in conjunction with the CISA Review Manual 2010.

To assist candidates in maximizing study efforts, questions are presented in the following two ways:
• Sorted by job practice area
• Scrambled as a sample 200-question exam

QAE-10 English Edition
QAE-10I Italian Edition
QAE-10J Japanese Edition
QAE-10S Spanish Edition

CISA Review Questions, Answers & Explanations Manual 2010 Supplement
ISACA

Developed each year, the CISA® Review Questions, Answers & Explanations Manual 2010 Supplement is recommended for use when preparing for the 2010 CISA exam. This supplement consists of 100 new sample questions, answers and explanations based on the current CISA job practice areas, using a process for item development similar to the process for developing actual exam items. The questions are intended to provide CISA candidates with an understanding of the type and structure of questions that have typically appeared on past exams, and were prepared specifically for use in studying for the CISA exam.

QAE-10ES English Edition
QAE-10FS French Edition
QAE-10IS Italian Edition
QAE-10JS Japanese Edition
QAE-10SS Spanish Edition

CISA Practice Question Database v10
ISACA

The CISA® Practice Question Database v10 combines the CISA Review Questions, Answers & Explanations Manual 2010 with the CISA Review Questions, Answers & Explanations Manual 2010 Supplement into one comprehensive 900-question study guide. Sample exams with randomly selected questions can be taken and the results viewed by job practice, allowing for concentrated study one area at a time. Additionally, questions generated during a study session are sorted based upon previous scoring history, allowing CISA candidates to easily and quickly identify their strengths and weaknesses and focus their study efforts accordingly.

Other features provide the ability to select sample exams by specific job practice areas, view questions that were previously answered incorrectly and vary the length of study sessions. The database software is available in CD-ROM format or as a download.

PLEASE NOTE the following system requirements:
• 400 MHz Pentium processor or equivalent (minimum); 1 GHz Pentium processor or equivalent (recommended)
• 512 MB RAM or higher
• One hard drive with 250 MB of available space (flash/thumb drives not supported)
• Mouse
• CD-ROM drive

CISA Online Review Course
ISACA

A complete web-based exam review course is available at www.isaca.org/elearning.
Adopting an Integrated Framework in Managing Fraud Risks

In September 2009, the Public Company Accounting Oversight Board (PCAOB) published a report on the first-year implementation of Auditing Standard No. 5 (AS5) in an audit of internal controls over financial reporting. AS5 was adopted in 2007 with the intent to guide auditors in performing more risk-based, top-down audits in complying with the US Sarbanes-Oxley Act. In reviewing more than 250 audits performed by eight of the largest US public accounting firms, the PCAOB inspectors found that areas that merited improvement include risk assessment, consideration of fraud, entity-level controls and deficiency evaluation. Specific findings encompassed inadequate attention to risks arising from IT general controls (ITGCs), failure in identifying compensating controls that mitigate areas susceptible to fraud risk and inappropriate conclusions made on the severity of control deficiencies identified.1

These findings are especially poignant in today’s challenging economic times when organizations face heightened risks of fraud and cost cutting and layoffs create opportunities for asset misuse. That said, tried and true IT audit practices can go a long way in helping organizations better manage risks. To this end, this article presents an integrated risk assessment framework for IT auditors to scope and execute targeted audits that better address areas of heightened risk, identify pervasive issues and assist organizations in improving their overall risk profiles over time. While focused specifically on IT risks, the integrated risk assessment framework addresses the three elements of the fraud triangle described in the Statement on Auditing Standards No. 99 (SAS 99), Consideration of Fraud in a Financial Statement Audit. In examining four key risk factors— inherent susceptibility, keys to the kingdom, process maturity and organizational maturity—the framework can be a useful tool in identifying opportunities for fraud, such as an absence of effective internal controls; incentives for fraud such as adverse relationships between employees and companies; and rationalization of fraud, such as ineffective communication of ethics.

**INHERENT SUSCEPTIBILITY**

From a Sarbanes-Oxley compliance perspective, it is second nature for management and auditors to identify systems and data with financial reporting impact. In reviewing for inherent susceptibility to fraud, however, this view can be self-delimiting and may not account for the myriad ways in which an asset may be stolen or misused. Loss of intellectual property resulting from theft of source code or loss of competitive advantage arising from stolen customer data are some of the areas that IT auditors should consider in today’s economy. Industry surveys show that, faced with job uncertainties, employees are more likely to steal or misappropriate company assets. Privileged users with access to critical computing infrastructure such as computer networks and servers are another source of risk that merits concern. Consider a real-life incident in which a systems administrator planted a logic bomb on his/her company’s computer network and purchased a significant amount of put options for the company stock in anticipation of a stock price decline accompanying the damage. The logic bomb ended costing the company more than US $3 million in remediation efforts.2

Thus, in reviewing an asset’s inherent susceptibility to fraud, it is useful to look beyond conventional financial system or data precepts. The former does not account for the full spectrum of ways in which stolen or modified assets can be misused. The latter may not take into consideration the sheer enormity of damage that can result from illicit modifications of pervasive computing infrastructure accessible to a set of privileged users but not exclusive to any specific category of corporate data. With these considerations in mind, mundane ITGCs such as access controls are cast in a new light. Depending on the level of the assessed risk, IT

1. In September 2009, the Public Company Accounting Oversight Board (PCAOB) published a report on the first-year implementation of Auditing Standard No. 5 (AS5) in an audit of internal controls over financial reporting. AS5 was adopted in 2007 with the intent to guide auditors in performing more risk-based, top-down audits in complying with the US Sarbanes-Oxley Act. In reviewing more than 250 audits performed by eight of the largest US public accounting firms, the PCAOB inspectors found that areas that merited improvement include risk assessment, consideration of fraud, entity-level controls and deficiency evaluation. Specific findings encompassed inadequate attention to risks arising from IT general controls (ITGCs), failure in identifying compensating controls that mitigate areas susceptible to fraud risk and inappropriate conclusions made on the severity of control deficiencies identified.

2. These findings are especially poignant in today’s challenging economic times when organizations face heightened risks of fraud and cost cutting and layoffs create opportunities for asset misuse. That said, tried and true IT audit practices can go a long way in helping organizations better manage risks. To this end, this article presents an integrated risk assessment framework for IT auditors to scope and execute targeted audits that better address areas of heightened risk, identify pervasive issues and assist organizations in improving their overall risk profiles over time. While focused specifically on IT risks, the integrated risk assessment framework addresses the three elements of the fraud triangle described in the Statement on Auditing Standards No. 99 (SAS 99), Consideration of Fraud in a Financial Statement Audit. In examining four key risk factors— inherent susceptibility, keys to the kingdom, process maturity and organizational maturity—the framework can be a useful tool in identifying opportunities for fraud, such as an absence of effective internal controls; incentives for fraud such as adverse relationships between employees and companies; and rationalization of fraud, such as ineffective communication of ethics.
auditors may choose to increase the depth of testing in areas that are deemed especially susceptible to fraud. In a retail environment, this may mean an increased focus on point-of-sale technology. In a high-tech environment, this may mean identifying key infrastructure that has pervasive impact and privileged users who have access to these systems.

KEYS TO THE KINGDOM

Users who have privileged access have the ability to create an unauthorized account, access an existing shared account or compromise an existing account belonging to a different user. In addition, unlike end-user accounts, privileged users often share generic system accounts that are manufacturer-supplied by default, whether these are operating system root accounts or database administrator accounts. As a result of an ongoing trend toward IT outsourcing as a means to cut costs, privileged users increasingly take on the face of temporary employees, contractors, consultants and business partners—groups that are expected to have a lesser degree of loyalty to an organization when compared to internal employees.

Perhaps what matters more is not the depth of access granted in any one singular system, but the breadth of access granted. Access to any one system may not raise a red flag, but when aggregated in an enterprisewide view across multiple systems, it may be a cause of concern. Therein lies the rationale for the implementation of least privilege, minimal access to resources to perform one's job. Segregation of duties, in the form of a role-based access control, is not a new concept—neither are controls over privileged accounts or passwords, for that matter. Still, it is not a sufficient deterrent against insider fraud. Pervasiveness of access across functions can be attained through collusion with another. In a review of insider cases associated with financial gain, the Computer Emergency Response Team (CERT) found that one-third of the cases of theft of information and half of the cases of modification of information involved collusion with at least one other insider.

In reviewing the nature of access to key assets, one cannot help but return to the basics of IT audit. Who holds the keys (privileged users, temps, contractors or business partners), where the keys are located (unknown backdoor accounts), when the keys are changed (password changes), what keys are available to an individual at any given time (pervasive access across systems) and how the keys are used (collusion either with another insider or an external party) are some of the questions that need to be tackled. In a highly outsourced IT environment, IT auditors may choose to prioritize the testing of third-party controls such as account provisioning and service-level monitoring. In a smaller company environment in which root access to key systems is held by one or selected administrative users, more attention may be required of generic system accounts and frequency of password changes. In a larger organization, a single sign-on solution may come under scrutiny for its potential to unlock excessive system access with a single unauthorized account.

PROCESS MATURITY

A robust business process possesses the requisite checks and balances (or segregation of duties) that precludes any one individual from taking a transaction from start to finish without an additional pair of eyes. In assessing risks associated with transaction processing, auditors invariably perform an end-to-end review of key classes of transactions, examining the mix of upstream vs. downstream, automated vs. manual controls that impact accuracy, completeness and validity. Opportunities for fraud arise in part from the absence of these business controls. In 2008, news broke about a trader at a European bank who leveraged his former position at the risk management office to execute a series of fictitious transactions that cost the bank more than US $7 billion. A contributing factor includes a lack of controls over trade cancellation and trader supervision.

The absence of process-level IT controls also gives rise to opportunities for fraud. Timely user deprovisioning, or the lack thereof, recurs time and again in numerous fraud incidents. At first glance, this seems obvious. If a user is no longer employed with an organization, why is access not disabled? In peeling back the layers, additional complexities await:

- If the user had privileged access to one or more systems—applications, operating systems, networks, servers, databases—the straightforward act of access disabling can become an administrative nightmare.
- What of backdoor accounts that the organization may not be aware of?
- Putting privileged access aside, what if there was a lag from the time the user was terminated to the time human resources (HR) was notified?
• What about a lag from the time HR was notified to the time a request was made to IT to disable access?
• What if IT incorrectly end-dated the terminated user’s enterprise resource planning (ERP) account in preserving referential integrity?
• What if IT were too caught up in other, more pressing endeavors to disable access on a timely basis?

These questions and more surface the everyday realities that organizations face.

Inadequate user access procedures are not the only culprits that may give rise to fraud. More recently, software development life cycle (SDLC) procedures have come under scrutiny. Besides a possible compromise in data confidentiality resulting from an absence of controls over the use of live production data for testing, other SDLC-related risks that can arise include the introduction of trapdoors in new or modified code from a lack of code review. Seen in this light, the importance of IT change management controls is underscored. If software development is an emerging focus, the maturity of system and network monitoring processes have been traditional areas of concern. A plethora of tools exists in the market, including intrusion detection systems (IDS), configuration controls, security incident event management (SIEM) systems and data loss prevention (DLP) technologies. Yet, for all the hoopla surrounding real-time data capture and exception alerts, the devil is in the details when it comes to the implementation and maintenance of ongoing monitoring mechanisms. Put simply, the mere existence of audit logs is not a control; the review is. A straightforward yet targeted tracking of suspicious File Transfer Protocol (FTP) downloads from a key server may yield more rewards than a false sense of security derived from automated signature updates.

Inadequate backup procedures have been another area of concern. In February 2008, an unencrypted backup tape went missing from a financial institution containing Social Security numbers and bank account information on 4.5 million customers. Despite several high-profile data leaks due to missing or stolen tapes over the years, many organizations fail to encrypt backup tapes. With backup-to-disk and online backup services replacing tape as the traditional medium of choice, encryption remains a key control in mitigating data breach risks. Gaps in backup procedures can also hinder an organization’s ability to recover from data loss. CERT described a case in which the restoration of deleted files failed, not because of corrupted backup, but rather from a lack of backup testing in ensuring that data were properly recorded.

The absence of process-level business and IT controls gives rise to opportunities for fraud. In assessing fraud risks from a process perspective, areas to consider include the adequacy of checks and balances in key business processes, as well as the maturity of IT processes in user provisioning, development, monitoring and backup. The frequency of business controls that are tied to specific application, i.e., application controls, can be invariably high and depends on the number of transactions processed. Conversely, ITGCs in IT processes have a lower frequency, e.g., monthly, but may have a higher impact due to the underlying pervasive infrastructure. These considerations impact the amount of work to be performed for the IT audit. IT auditors need to audit where it truly matters (pervasive impact), but also determine the level of sampling necessary to obtain a level of comfort that the controls are operating effectively. The IT processes covered here merely scratch the surface. Other processes that merit further analysis include patch and configuration management. On the former, just as it may be a time-consuming process for organizations to disable all forms of privilege associated with a terminated user, it can be challenging to release security patches to key servers on a timely basis, especially if these are not all configured in the same manner. On the latter, even if organizations do not develop their own software, they need to pay attention to fraud risks arising from unchanged default configurations that come with a commercial off-the-shelf (COTS) program or Software as a Service (SaaS).

ORGANIZATIONAL MATURITY
Often, an over-focus on transaction or system minutiae, whether it be process approvals, system logins or configurations, fails to take into account the overall organization environment. An absence of overarching company or entity-level controls gives rise to opportunities for fraud. Entity-level controls such as security policy definition, timely update and periodic communication can go a long way toward mitigating risks arising from employee malice or negligence. Lack of security awareness, for instance, has been a key contributor to social engineering attacks. Users visiting web sites or receiving e-mail may be fooled into downloading malicious code. IBM’s ISS X-Force division reported greater sophistication in phisher attacks with the most popular subject lines comprising merely 6.25 percent of all phishing e-mails.

Another entity-level control to assess is preemployment background screening. Preemployment background screening has been traditionally performed for finance and accounting hires. To the extent that all insiders in a CERT study on IT sabotage exhibited personal predispositions, consideration should be given to prescreening IT hires who have privileged
access to key systems with pervasive impact. As an entity control, preemployment background screening can be useful in detecting any personal dispositions to fraud. In studying the psychology of the dangerous insider, the authors of “The Insider Threat to Information Systems; Psychology of the Dangerous Insider” describe the interplay among personal vulnerabilities, situational stress and the organization environment.10

The old adage “no smoke without fire” comes to mind. Fifty-seven percent of insiders in a joint US Secret Service and CERT study were called out for inappropriate behavior in the workplace prior to performing the insider incidents.11 The availability of avenues in an organization for reporting and addressing employee concerns or issues has an important bearing on how it in turn responds to insider risks. In analyzing compliance hotline reports from 1,328 organizations, the Network and BDO Consulting found that the reporting of fraud-related incidents increased from 10.9 percent of all complaints in the first quarter of 2006 to 21 percent in 2009.12 Whether formalized in whistle-blower procedures in support of the organization’s code of ethics or documented as part of general supervisor responsibilities, the reporting and handling of workplace issues cannot be underestimated. While the system monitoring of suspicious activities can be akin to finding a needle in a haystack, following up with reported issues in the workplace may very well avert a likely insider attack.

In assessing the maturity of entity-level controls, security policies and awareness, preemployment screening and avenues for reporting and handling workplace issues are all potential areas to review. Other areas that have not been covered in this article but are worth exploring further include the placement, alignment and effectiveness of the internal audit function within the organization. In reviewing the nature of entity-level controls within an organization, the IT auditor can make better decisions on the level of reliance on entity-level controls and correspondingly the level of testing to be performed on process-level controls.

INTEGRATED FRAMEWORK

In forming an integrated risk assessment framework, IT auditors need to appreciate the different interplay between two or more risk factors. Figure 1 provides a recap of various risk factors associated with fraud. Pervasiveness of access across applications in a smaller company, for example, may be compensated by an effective set of checks and balances in key business processes. On the other hand, tightened user provisioning and monitoring in a different organization may be undermined by an overall lack of employee awareness of security policy or social engineering threats. Similarly, the value of continuous system monitoring may be diluted by relaxed provisioning over system or database administrators who have the ability to modify audit logs. More important, multiple risk factors can combine to form a trajectory toward fraud.

Consider the following scenario:

- An organization prioritizes key system and data as part of its overall enterprise risk management, but does not take into consideration selected individuals with privileged access.
- The internal system environment is characterized by multiple shared-privileged accounts on various platforms.
- While checks and balances exist for business processes, IT processes in user provisioning and monitoring remain weak.
- Entity-level controls reflect gaps in awareness of security policies with preemployment screening conducted for finance and accounting hires only.
- After a recent round of layoffs, the organization increases its level of reliance on temps and contractors for IT support.

In this scenario, each individual observation may not be a cause of concern, but combined, they form a predisposing condition for fraud. This is a pervasive issue that IT auditors need to highlight for management. Rather than provide an itemized list inventorying a hodgepodge of seemingly unrelated concerns, IT auditors need to stand back and keep management apprised of the big picture. An integrated perspective leads to well-informed management decisions. In assessing its options, the organization may undertake a phased road map. That is, in the short term, it may prioritize controls over shared passwords associated with privileged accounts and access provisioning.
for IT temporary employees and contractors. **Figure 2** reflects corresponding improvements in the nature of access (keys to the kingdom) and IT process maturity. Over the long run, the organization may invest in security awareness programs for employees, temporary employees and contractors, as well as selected system monitoring tools that track privileged users. **Figure 3** reflects corresponding improvements in organizational maturity and IT processes.

**CONCLUSION**

The recent PCAOB report, on the one hand, indicates there is still progress to be made in performing risk-based audits that add value to an organization. Today’s uncertain economy, on the other hand, continues to challenge IT auditors to better assist organizations in managing fraud risk. In adopting an integrated risk assessment framework, IT auditors become better equipped in audit planning, execution and reporting in helping organizations mitigate fraud. By providing management with an insight into the interactions that can take place among one or more risk factors, IT auditors help management uncover systemic issues that truly matter. As processes, systems or people change, IT auditors play a key role in helping organizations revisit and adapt their risk strategies.

**ENDNOTES**


2 Business & Legal Reports Inc.; “IT Worker Sentenced to 8 Years in Prison for Computer Sabotage,” 28 December 2006, [http://hr.blr.com](http://hr.blr.com)


5 S. Allen; “Controls Lessons From the Société Générale Fraud: What Patterns Emerge From Rogue Trading Incidents of the Recent Past?,” *Banking Accounting & Finance*, 1 October 2008


7 *Op cit*, Cappelli, *et al*


12 The Network and BDO Consulting; *2009 Corporate Governance and Compliance Hotline Benchmarking Report*, USA, 2009
Many companies today are paying attention to cloud computing and new aspects of large-scale, distributed computing. This emerging paradigm of the information age offers exciting benefits to companies and users, but cloud computing, like any other innovation, faces challenges such as security and privacy risks.

How do different stakeholders perceive these risks and the effectiveness of the mitigations? And, how are these reflected in their trust in the cloud? The answers to these questions can affect the outcome of policy debates, and the allocation of resources in controlling security issues of cloud environments.

This article presents an introduction to the cloud and some of its advantages and disadvantages. It discusses the role of risk perception and trust in security and privacy challenges of the cloud. It also makes recommendations addressing these challenges.

**WHAT IS CLOUD COMPUTING?**

Just as clouds can take different shapes and be viewed differently, so too is cloud computing perceived differently. To some, the cloud looks like web-based applications—a revival of the thin client. To others, the cloud looks like utility computing—a grid that charges metered rates for processing time. To some, the cloud could be parallel computing, designed to scale complex processes for improved efficiency.\(^1\)\(^2\) Interestingly, cloud services are also wildly different. Amazon’s Elastic Compute Cloud offers full Linux machines with root access and the opportunity to run whatever apps the user chooses. Google’s App Engine will also let users run any program they want—as long as the user specifies it in a limited version of Python and uses Google’s database.\(^3\)

The National Institute of Standards and Technology (NIST) defines cloud computing as “a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.”\(^4\)

It is important to remember that the Internet is in fact a primitive transport cloud. People place something on the path with an expectation that it will get to the proper destination, in a reasonable time, with all parties respecting the privacy and security of the artifact.

**ADVANTAGES AND DISADVANTAGES OF CLOUD COMPUTING**

Cloud computing brings many advantages to users and vendors. One of its biggest advantages is that a user may no longer have to be tethered to a traditional computer to use an application, or have to buy a version of an application that is specifically configured for a phone, personal digital assistant (PDA) or other device. It is likely that, at some point, any device that can access the Internet will be able to run a cloud-based application. Application services are available independent of the user’s devices and network interfaces. Regardless of the device being used, users also face fewer maintenance issues. Users will not have to worry about storage capacity, compatibility or other similar concerns.

From a technical standpoint, these benefits are the result of the distributed nature of the web, which necessitates a clear separation between application and interaction logic. This is because application logic and user data reside mostly on the web cloud and manifest themselves in the form of tangible user interfaces at the point of interaction, e.g., within a web browser or mobile web client.\(^3\)

Cloud computing also seems to be beneficial for vendors. Businesses frequently find themselves using the vast majority of their computing capacity in a small percentage of time, leaving expensive equipment often idle. Cloud computing can act as a utility grid for vendors and optimize the use of their resources.

Consider, for example, a web-based application running in Amazon’s cloud. Suppose...
there is a sudden surge in visitors as a result of media coverage, for example. Today, many web applications fail under the load of big traffic spikes. But in the cloud, assuming that the web application has been designed intelligently, additional machine instances can be launched on demand. The application dynamically and gracefully scales up. When traffic slows down, the application can scale down, terminating the extra instances.

For small businesses, this means that new storage and processing capacity can be added incrementally, instead of necessitating the purchase of a whole new server at a time. For larger and distributed companies, where the team members all work from their own homes or different locations, it makes coordination, document sharing and collaboration a lot easier. Amazon, Google and EMC are examples of large vendors that have welcomed cloud computing and have invested in developing the IT infrastructure that the cloud computing environment requires.

However, there are some downsides to the cloud. The problems that the IT community has experienced with large, distributed systems may apply to cloud environments as well. For example, a cloud’s use is contingent on accessing the Internet and the cloud servers. What should users do if some servers fail to operate and data are not accessible, e.g., when Amazon’s cloud services suffered a service outage for several hours and did not return to normal until about eight hours after the problem first occurred in early July 2009? What are the chances of similar outages in the future? This highlights the current immaturity of cloud computing. How long will it take to identify the problem, analyze it and respond to it? What liability does a company face when there has been a security breach in the cloud? Considering these potential problems, how can users trust the cloud?

Some security managers believe that security and privacy issues over cloud computing are not very different from those surrounding any sort of IT outsourcing, but others believe that there are specific security and privacy risks to cloud computing. For example, Siani Pearson explains that “cloud computing enables new services to be made available in the cloud by combining other services. For example, a ‘print on demand’ service could be provided by combining a printing service with a storage service. This procedure of service combination is typically under less control than previous service combinations carried out within traditional multiparty enterprise scenarios.”

The results of a recent survey indicate that many business and IT managers see potential value in the cloud, but fears over security and control are holding them back. By a five-to-one margin, managers who participated in this survey felt that their own IT systems are more secure than the cloud. These results clearly indicate that fears about security and control of data are limiting the cloud’s broad adoption.

In addition, there have been some notable security incidents in cloud environments that may make potential cloud users think twice before adopting cloud computing. For example, in March 2009, a system error within Google Docs allowed the contents of private documents to be exposed to the public for a brief period of time. As a result, the Electronic Privacy Information Center (EPIC) filed a complaint with the US Federal Trade Commission, requested an injunction against Google and claimed Google’s inadequate security is a deceptive business practice.

**SECURITY AND PRIVACY’S INFLUENCE ON TRUST**

Currently, there are two broad categories of cloud computing:
1. Online applications, such as Google’s Apps, Yahoo’s Zimbra for e-mail, Zoho for office and business software, Adobe Buzzword for word processing, and Salesforce.com for managing customer relations
2. General-purpose foundations, such as Amazon Web Services, Salesforce.com’s Force.com and Google App Engine on which customers can run their own applications

How do users trust this new computing environment?

Distrust is one of the main constraints on online environments, particularly in terms of consumer protection. Although the elements that contribute to building trust can be identified in broad terms, there are still many uncertainties in defining and establishing trust in online environments.

Why should users trust cloud environments to store their personal information and to share their privacy in such a large and segregated environment?

This question can be answered only by investigating these uncertainties and by exploring the relationship between trust and the way in which the risk is perceived by stakeholders.

Users are assumed to be willing to disclose personal information and have that information used subsequently to store their personal data or to create consumer profiles for business use when they perceive that fair procedures are in place to protect their individual privacy. Individuals are
less likely to be dissatisfied even with unfavorable outcomes if they believe that the procedures used to derive those outcomes are fair.

In general, individuals are less likely to perceive information collection procedures as privacy-invasive when:
- Information is collected in the context of an existing relationship
- They perceive that they have the ability to control future use of the information
- The information collected or used is relevant to the transaction
- They believe the information will be used to draw reliable and valid inferences about them

Creating a willingness in consumers to disclose personal information, then, requires that organizations manage the second exchange strategically. Consumers should continue to disclose personal information on cloud environments as long as they perceive that they receive benefits that exceed the current or future risks of disclosure. Creating willingness in consumers to disclose personal information requires that the second exchange be based on a fair social contract.

How do users perceive security and privacy risks in cloud environments?

CHARACTERIZING PERCEPTIONS OF SECURITY AND PRIVACY RISKS

Whereas technologically sophisticated analysts employ risk assessment to evaluate hazards, the majority of citizens rely on intuitive risk judgments, typically called “risk perceptions.” For those people, experience with hazards tends to come from news media, which rather thoroughly document mishaps and threats occurring throughout the world.10

As experience shapes user perceptions, they become proxies of actual risk that may be good predictors of risk in the absence of better methods. Even if this is not a precise process, sound management practice dictates that user perceptions of risk be addressed as part of a total risk management approach. Traditional methods of IT risk assessment do not consider risk perception as either a predictor of risk nor as a factor that should be addressed in preventing misuse.

Cloud privacy risks are also perceived differently by different cloud stakeholders. Pearson categorizes four types of perspectives for privacy risks in cloud environments:11
- **Cloud service users**—Being forced/persuaded to give personal information involuntarily
- **Organizations using the cloud service**—Noncompliance to enterprise policies and legislation and/or loss of reputation and credibility
- **Implementers of cloud platforms**—Exposure of sensitive information stored on the platforms, loss of reputation and credibility
- **Providers of applications on top of cloud platforms**—Legal noncompliance, loss of reputation and “function creep” using the personal information stored on the cloud

Baruch Fischoff and his colleagues investigated perceptions of technology risks, and particularly ways to determine when a product is acceptably safe. Their model can be adapted by companies that are considering operating in clouds to define risk perception of their users, and includes:12

1. **Voluntariness**—Does the user voluntarily get involved in the cloud?
2. **Immediacy of effect**—To what extent is the risk of consequence from the cloud user’s actions immediate?
3. **Knowledge about risk**—To what extent are the risks known (precisely) by the cloud user who is exposed to those risks?
4. **Knowledge of science**—To what extent are the risks precisely known and quantified?
5. **Control over risk**—To what extent can the cloud user, by personal skill or diligence, avoid the consequences to him/her while engaging in untoward activity?
6. **Chronic or catastrophic**—Does the risk affect the cloud user over time, or is it a risk that affects a larger number of people at once?
7. **Newness**—Are these risks new to the cloud user or is there some prior experience/conditioning?
8. **Common dread**—Is this a risk that the cloud user has rationalized and can think about reasonably calmly?
9. **Severity of consequences**—When is the risk from the activity realized in the form of consequences to the user?
It has been shown that unknown risk and fear can be used to account for about 80 percent of the results generated by using all nine variables that were originally introduced by Fischoff and his colleagues. The author of this article formulated a model based on the models of risk perception developed by Fischoff, Slovic and others, in which characteristics of a risk are correlated with its acceptance. The model was modified to condense Fischoff’s nine variables of risk, by considering understanding (familiarity and experience) and consequences (scope, duration and impact) to the stakeholder, into the two principal characteristics of information security and privacy risks, as shown in figure 1.

For the first dimension of the model, addressing consequences of the breach, scenarios can be posited to explore the fear cloud users have of the potential effects of the risk of information security losses. By exploring the fear cloud users have of the potential effect to them of perpetrating IT misuse, the consequences of the breach can be modeled. To model this, three categories of questions are considered, as described in figure 2.

Analyzing these questions enables one to assign a simple metric to this dimension of the model. The five levels of consequence are as follows:
1. Effects are trivial, temporary and commonplace.
2. Effects are potentially serious but treatable/recoverable.
3. Effects are serious and long-term but considered normal.
4. Effects are serious, ongoing and raise deep concerns.
5. Effects are catastrophic, ongoing and highly feared.

The level definitions (“trivial,” “serious,” etc.) are based on those published by NIST. Level 5 and level 1 represent the highest and lowest level of consequences to stakeholders, respectively.

For the second dimension, understanding, the factors motivating cloud users to consider certain risks while dismissing others can be explored. These questions are intended to identify effective factors that influence users’ cognitive understanding of cause and effect. This results into two main categories of questions as described in figure 3.
This framework for categorizing understanding is based on the work of Bloom and Krathwhol. The goal is to understand the risk causes and effects using the cognitive domain and what adds to cloud users' motivation to increase the understanding using the affective domain. The following six levels were obtained for the understanding dimension of the model:

1. Evaluation—Can the cloud user make judgments about the value of ideas or materials?
2. Synthesis—Can the cloud user build a structure or pattern from diverse elements?
3. Analysis—How do cloud users distinguish between facts and inferences?
4. Application—How do cloud users use a concept in a new situation or unprompted use of an abstraction?
5. Comprehension—Can cloud users understand the problem, i.e., state a problem in their own words?
6. Knowledge—Can the cloud user recall data or information?

Level 6 and level 1 represent the lowest and the highest level of understanding, respectively. The perceived risk in the model is a function of consequence and understanding. An approximate perceived risk score may be constructed from the consequence metric and the inverse of the understanding metric. The perceived risk score, therefore, increases whenever the consequences are more severe for stakeholders and decreases as stakeholders gain a deeper understanding of the nature and limits of the risk. Some cases may not match this model exactly, but this score is nonetheless a good match for many case studies and the experiences of the experts interviewed in the author's validation study.

For example, imagine that the identity of a cloud user has been stolen as a result of being in a cloud environment. As the first incident occurs, the cloud user's understanding is low at first—levels 5 and 4 of the U dimension. Understanding increases with time and reaches a maximum—levels 2 and 1. Thereafter, there is little increase for subsequent incidents. Typically, there may be a sudden increase in consequences—from level 2 to level 4 of the C dimension, which may either grow or decrease with time depending on the kind of fraud perpetrated. Privacy loss may increase with time as the victim is required to expose more details to recover, but eventually the loss subsides to a steady state of lasting privacy loss.

Research findings also indicate that perceived benefit lowers the perceived risk of electronic activities; when one stands to gain a great deal from a certain activity, one is likely to underestimate the risks involved in the activity.

**WHAT IS NEXT FOR CLOUD?**

“If you’re a large enterprise, somebody in your organization is using cloud computing, but they’re not telling you,” says James Staten, principal analyst at IT adviser Forrester Research. “So there’s a good chance that in the next five years, you’re going to inherit things that were born in the cloud anyway, and now you’ll have to manage them.”

Merrill Lynch estimates that within the next five years, the annual global market for cloud computing will surge to US $95 billion. In a May 2008 report, Merrill Lynch estimated that 12 percent of the worldwide software market would go to the cloud in that period.

These statistics should come as no surprise. Well over 90 percent of information currently produced is created in a digital format, and this percentage is anticipated to increase substantially in the future.

Dealing with such a vast amount of information in such a format requires means of large-scale, distributed computing such as cloud. But, the missing piece is the legal infrastructure and management that will provide the incentives to make such access economically viable. This missing piece is a source for concern for managers regarding compliance with regulations, e.g., the US Sarbanes-Oxley Act, which governs corporate financial reporting, and the US Health Insurance Portability and Accountability Act (HIPAA), which sets rules for security and privacy of health records. For example, ITricity, a European provider of cloud computing capacity, previously could not offer services to companies that required compliance with financial and health care regulations.

**ADDRESSING PRIVACY AND SECURITY RISKS WITH CLOUD COMPUTING**

Risk mitigation in cloud environments is not simple. It depends on complex technical and human factors. Despite this complexity, it is possible to sufficiently understand risk causes and controls in order to apply cost-effective controls.

**Understanding Technical Vulnerabilities**

Technical controls continue to be important, especially when an organization is coping with outsider attacks and unexpected failures. Collaboration among experts from industry, academia and government would result in providing better security solutions. For example, a solution that was recently discussed among a panel of academic and industry experts was to enable security and reliability services by virtue
of being located in the cloud.\textsuperscript{20} As described by John Oberheide, Evan Cooke and Farnam Jahanian, providers and implementers can use a cloud-based antivirus solution that can not only utilize multiple vendors to provide better coverage, but also compares data blocks across users to improve efficiency and provide an archival service for forensic analysis.\textsuperscript{21}

ISACA considers addressing transparency, privacy, compliance, transborder information flow and certification key assurance issues for cloud computing.\textsuperscript{22} ISACA also argues that standards (existing or new ones that may be developed for the cloud computing paradigm) should be consulted to address the relevant areas, and businesses should look to adjust their existing control frameworks. A literature review identifies some efforts in developing best practices and standards for cloud computing made by NIST and the Cloud Security Alliance.\textsuperscript{23}

At the time of writing, there is no comprehensive and commonly accepted standard to address the technical risks in cloud environments. There does exist, however, a hierarchy of approaches such as checklists and scenario generation techniques that require the user to have only a minimum knowledge of information systems security. To have a well-defined scope for the checklist, cloud managers can follow the formats that are provided by British Standards or the US National Security Agency (NSA). The NSA suggests using 18 areas for information security assessment, which is more comprehensive than the British Standards. It is suggested to follow the NIST’s guidelines for ranking threats, use NSA’s 18 areas of information security assessment, and use checklists for vulnerability assessments that can lead an organization to estimate probabilities of the occurrence of incidents and quantify information security risks.\textsuperscript{24}

Stakeholder Involvement
Control security issues and economic decision making about cloud environments without consideration of trust and risk is not likely to be optimal. High trust can result in lower cost, higher efficiency, minimal contracting and minimum transaction monitoring. Indeed, a high level of trust enables a high level of risk taking, because trust is the mirror image of risk; high trust suggests low perceived risks.\textsuperscript{25} For example, long-term trading partner relationships can be sustained via positive trust. However, the use of power among trading partners may influence trust for only a short period of time. Thus, cloud managers can acquire and use power effectively and positively to meet goals and improve the likelihood of success, at least for maintaining trading partner relationships, particularly online.

Alongside the consulting standards and technical analysis of options available to reduce cloud risks, cloud managers should take explicit steps to involve the stakeholders—to understand what they are concerned about and why and to communicate good information about risk, targeted to the needs of stakeholders. For example, in the UK, Her Majesty’s Treasury uses a framework for understanding people’s concerns about different technologies so they can be considered in policy development and in the development of related consultation arrangements and communication strategies.\textsuperscript{26} This model is based on the risk perception models that were discussed previously, in which characteristics of risk are correlated with its acceptance. For example, risks that are undertaken voluntarily are generally considered more acceptable than risks that are imposed without consent. Similarly, risks that cause fear are also considered to be less acceptable.

Cloud managers can learn from this analysis of previous research on users’ perceptions of risk of different technologies by being aware of the likely effects of risk perception on the acceptance and implementation of proposed policies. At the same time, cloud managers can acknowledge the active role of users in online environments—a role that differentiates information technology from many other technologies. In cloud environments, users actually operate the technology. This hands-on aspect of online interaction affects key aspects of risk, such as knowledge and control. For these reasons, cloud managers should consider user perceptions of risk when establishing trust with their customers.

The Gartner Group has specified seven cloud computing security risks to users:\textsuperscript{27}

1. **Privileged user access**—Outsourced services bypassing the physical, logical and personal controls IT shops exert over in-house programs
2. **Regulatory compliance**—Users being ultimately responsible for the security and integrity of their own data, even when the data are held by a service provider
3. **Data location**—Users not knowing where their data are stored
4. **Data segregation**—Data in the cloud being in a shared environment alongside data from other customers
5. **Recovery**—Fuzziness about ability to do a complete restoration and the time it takes
6. **Investigative support**—Difficulties in investigating inappropriate or illegal activities
7. **Long-term viability**—Availability of data in their original format after procedural and technical changes in the cloud environment
To establish trust with users in the cloud environment, organizations should address these risks. They also need to align their users’ perceptions with their policies. Efforts should be made to develop a standardized approach to trust and risk across different domains to reduce the burden on consumers who seek to better understand and compare policies and practices across these organizations. This standardized approach will also aid organizations that engage in contractual sharing of consumer information, making it easier to assess risks across organizations and monitor practices for compliance with contracts, policies and law.

Individual customers expect a given activity in which they participate to be conducted fairly and to address their privacy concerns. By ensuring this fairness and respecting privacy, organizations give their customers the confidence to disclose personal information on the cloud and to allow that information subsequently to be used to create consumer profiles for business use.

Thus, organizations that understand the roles of trust and risk should monitor user perceptions to understand their relation to risk aversion and risk management. Managers should not rely solely on technical control measures. Security researchers have tended to focus on the hard issues of cryptography and system design. By contrast, issues revolving around the use of computers by lay users and the creation of incentives to avoid fraud have been relatively neglected. Many studies have shown that human errors are the main cause of information security incidents.28

**Conclusion**

Piecemeal approaches to control security issues of cloud environments fail simply because they are usually driven by a haphazard occurrence, the most recent incident or the most recently publicized threat. In other words, managing information security in cloud environments requires collaboration among experts from different disciplines, including computer scientists, engineers, economists, lawyers and policy makers, to forge common approaches.

**Endnotes**

1 Hoover, J. N.; R. Martin; “Demystifying the Cloud,” InformationWeek, June 2008
11 *Op cit*, Pearson
24 Ibid.
26 Her Majesty’s Treasury, “Managing Risks to the Public: An Appraisal Guidance,” UK, 2005

EDITOR’S NOTE
ISACA recently released the Cloud Computing: Business Benefits With Security, Governance and Assurance Perspectives white paper. It is available to the public as a complimentary PDF download from www.isaca.org/cloud. To learn more about ISACA research projects in development, please visit www.isaca.org/research.

The 2010 Information Security and Risk Management Conference, held in both Las Vegas, Nevada, USA and Vienna, Austria, will offer multiple sessions related to cloud computing. Learn more about these opportunities at www.isaca.org/ism.
By Myles Mellor
www.themecrosswords.com

ACROSS
1 One part of CIA
6 Service (updates and fixes)
9 Philosopher who described a dual reality
10 Free tool that can be used to assess Payment Card Industry
    DSS compliance for wireless access points
12 Bank routing number abbreviation
14 Red carpet visitor
15 Observe closely
17 Writer of “Pieces of the Puzzle,” William ____
18 Underlined, for short
20 Trendsetting
22 Represent
25 ____ on the board
29 Tampa locale
30 One step in the escalation of a fraudster
34 Yale student
35 Milliliter, abbr.
36 Tools to identify, correct and standardize incomplete and
    inconsistent source information prior to loading to data
    warehouses, abbr.
38 This can lead to the detection of fraud.
42 Provided that
44 Chinese dollar
45 Quote a source
47 Separation
48 Careless
50 Abbreviation for systems that will detect intrusion into
    data systems

DOWN
1 Put into effect
2 Follow a paper trail, e.g.
3 Universal
4 In a perfect world
5 365 days for short
6 Cousin to confidentiality
7 Enforces
8 Internet location
11 Transgression
13 Go see ____ fi movie
16 Believe
19 Most data warehouse initiatives use ___ tools to standardize the
    data transfer process, abbr.
21 “Is that so!”
23 Prep. test
24 Futures industry organization, abbr.
26 A big ____
27 Oddity that an auditor notices that can be the “tip of the
    fraud iceberg”
28 Antiquated piece of equipment, for example
31 Layer?
32 Come out on top
33 Trademark, abbr.
37 Search
38 Doctrine
39 One form of 52 across
40 Gold symbol
41 ____ hurry
43 Act relating to information security practices
46 Follow
49 Many assessment tools provide data in this output.
51 Modern courtroom evidence

52 ____ 70 is a defined standard developed by the AICPA
53 Cambridge Univ.
54 ____ solutions verify, balance, reconcile and track information
    as the source system data traverse through various points of the
    ETL process to the data warehouse, abbr.
55 Silvery metal symbol
56 Author of “Computer and Information Security Handbook,”
    John ____

(Answers on page 54)
CISM Review Manual 2010
ISACA

The ISACA® Review Manual 2010 is a comprehensive reference guide designed to assist individuals in preparing for the CISM exam and individuals who wish to understand the roles and responsibilities of an information security manager. The manual has evolved over the past six editions and now represents the most current, comprehensive, globally peer-reviewed information security management resource available.

The CISM Review Manual 2010 features a new format. Each of the five chapters has been divided into two sections for focused study. The first section contains the definitions and objectives for the five areas, with the corresponding tasks and knowledge statements that are tested on the exam.

Section 1 is an overview that provides:
- Definitions for the five areas
- Objectives for each area
- Descriptions of the tasks
- A map of the relationship of each task to the knowledge statements
- A reference guide for the knowledge statements, including the relevant concepts and explanations
- References to specific content in section 2 for each knowledge statement
- Sample practice questions and explanations of the answers
- Suggested resources for further study

Section 2 consists of reference material and content that supports the knowledge statements. Material included is pertinent for CISM candidates’ knowledge and/or understanding when preparing for the CISM certification exam. Also included are definitions of terms most commonly found on the exam.

This manual can be used as a stand-alone document for individual study or as a guide or reference for study groups and chapters conducting local review courses. It is a primary reference resource for information security managers seeking global guidance on effective approaches to governance, risk management, program development, management and incident response.

The 2010 edition has been developed and is organized to assist candidates in understanding essential concepts and studying the following job practice areas:
- Information security governance
- Information risk management
- Information security program development
- Information security program management
- Incident management and response

CM-10 English Edition
CM-10J Japanese Edition
CM-10S Spanish Edition

ISACA

The CISM® Review Questions, Answers & Explanations Manual 2009 consists of 450 multiple-choice study questions that have previously appeared in the CISM® Review Questions, Answers & Explanations Manual 2008 and the 2008 Supplement. These questions are not actual exam items, but are intended to provide CISM candidates with an understanding of the type and structure of questions and content that have previously appeared on the exam. This publication is ideal to use in conjunction with the CISM Review Manual 2010.

To assist candidates in maximizing study efforts, questions are presented in the following two ways:
- Sorted by job practice area
- Scrambled as a sample 200-question exam

CQA-9 English Edition
CQA-9J Japanese Edition
CQA-9S Spanish Edition

CISM Practice Question Database v10
ISACA

The CISM® Practice Question Database v10 combines the CISM Review Questions, Answers & Explanations Manual 2009 with the CISM Review Questions, Answers & Explanations Manual 2009 Supplement and 2010 Supplement into one comprehensive 650-question study guide. Sample exams with randomly selected questions can be taken and the results viewed by job practice, allowing for concentrated study one area at a time. Additionally, questions generated during a study session are sorted based upon previous scoring history, allowing CISM candidates to easily and quickly identify their strengths and weaknesses and focus their study efforts accordingly. Other features provide the ability to select sample exams by specific job practice areas, view questions that were previously answered incorrectly and vary the length of study sessions.

The database software is available in CD-ROM format or as a download.

PLEASE NOTE the following system requirements:
- 400 MHz Pentium processor or equivalent (minimum); 1 GHz Pentium processor or equivalent (recommended)
- 512 MB RAM or higher
- One hard drive with 250 MB of available space (flash/thumb drives not supported)
- Mouse
- CD-ROM drive

MDB-10 English Edition—CD-ROM
MDB-10W English Edition—Download
Gan Subramaniam, CISA, CISM, CCNA, CCSA, CIA, CISSP, ISO 27001 LA, SSCP, is the global IT security lead for a management consulting, technology services and outsourcing company’s global delivery network. Previously, he served as head of IT security group compliance and monitoring at a Big 4 professional services firm. With more than 16 years of experience in IT development, IS audit and information security, Subramaniam’s previous work includes heading the information security and risk functions at a top UK-based business process owner (BPO). His previous employers include Ernst & Young, UK; Thomas Cook (India); and Hindustan Petroleum Corp., India. As an international conference speaker, he has chaired and spoken at a number of conferences around the world.

Q

I recently read a wonderful book, *8 Things We Hate About IT: How to Move Beyond the Frustrations to Form a New Partnership with IT*. It made for an interesting read, listing out disconnects between the business and the IT function. The author gave a good deal of practical examples. The charm of the book was that the author, Susan Cramm, gave clear solutions to the illustrated problems.

I was wondering whether you can list out, in a similar manner, the ‘things we hate’ about IT security or information security. Please list them from your point of view (no compulsion to list eight). You may also wish to add what IT security must do in terms of making amends.

A

Very interesting question. I made it a point to buy that book (published by Harvard Business School Press) after reading your question and became an instant fan of it. It is extremely well written with a lot of practical examples and not just bookish theory, frightening the reader with jargon.

I do not have the luxury of writing a book on the subject and have the constraint of limiting my thoughts to this column, though your question is a good idea for a theme that could be developed into a book.

Let me try to extrapolate the same concept from an IT security point of view. I will tell you the other side of the story as well.

- **Whilst the business aims to achieve its objectives**, IT security throws a spanner in the wheel by imposing restrictions in the name of security policies that add little value to the overall business operations. IT security policies cannot be written for the sake of the survival and thriving of chief security officers and their cronies, but must be clearly aimed to minimise the real risks, not some illusionary risks. It must take into account the risks surrounding the business and work towards mitigating them.

- **Business wants IT security to focus on strategic business issues and align its goals towards the strategic issues**, whereas the IT security function ends up spending its efforts on operational issues with limited consideration of the bigger picture and long-term goals. Patching desktops that host no sensitive information, and sitting behind multiple layers of security, such as firewalls, intrusion detection systems or intrusion prevention systems, must be the least priority for IT security.

- **Allocated funding gets spent on bringing in unwanted technology solutions for geeks to play with**, rather than focusing on creating awareness amongst people who are the biggest purveyors and creators of risks. It is like buying an aircraft when all you need is a bicycle. The story is very old and well known: security viewed as a technology issue, rather than a people issue.

- **Security auditor, the devil within, is someone who wants everything to be audited for the sake of running a compliance and certification regime.** Not ferreting out the right issues, the audit may focus on trivial matters. Such audits may mislead the leadership on the state of affairs because the real issues that remain on the ground do not get identified and reported. The focus areas of the audits may remain wrong.

Let us look at the other side of the story:

- **Business wants to control IT security and its activities**, thereby stifling the real voice that can speak out certain ‘moments of truth’. IT security may lack independence of operations; perhaps due to undue influence, the business is able to influence in terms of reporting relationships. Doing this will lead to a scenario in which IT security is not able to voice its independent opinion on risks and controls and, thereby, is not able to choose its priorities to allocate resources appropriately.

- **Business focuses on collecting badges in the form of certifications and using IT security or information security as a vehicle to reach that destination, not realising that achieving security excellence is nothing but a continuous journey and never a destination.** Instead of using IT security to focus on key risks and controls, it gets used as a jewel in the showcase with an aim to earn undeserved laurels.
Business may want security incidents to go unreported or underreported. Fearing loss of reputation or potential regulatory issues, businesses may choose to underplay security incidents. Equally, some business leads that may end up controlling IT security due to organisational structure may choose to get unwanted and irrelevant incidents reported and justify the funding allocations using the traditional concept of ‘fear, uncertainty and doubt’.

On the audit front, the business may hide issues, pulling them under the carpet, and try to showcase an ‘all is well’ scenario, while knowing well that the hidden issues are endless. Unless a major incident hits, the business does not feel the pain. A multitude of incidents may happen, but something non-catastrophic may help the business to fob off auditors on actual incidents.

All said, what is required to bridge the gap, because in both scenarios the sufferers are the key stakeholders in the business—be it customers or shareholders? My illustrative list—as always non-exhaustive—is as follows:

- Business and IT security must work in complete partnership. This does not mean that IT security’s independence of operations must be compromised. The functions must define the boundaries and set the rules for co-existence.
- IT security must help business identify the real security risks that may impede it from achieving its objectives.
- Businesses should not live under any illusionary joy of a ‘no audit observations’ regime, which would really harm it in the long run. It must learn to recognise that audit observations are positive because they create opportunities for improvement.
- The ultimate decision to accept any risk must be that of the business. The ideal scenario would be for the IT security group to identify the right risks and to reasonably quantify or qualify the potential impacts should they materialise and for the business to make the right decision regarding accepting, mitigating or transferring the risk. In this ‘ideal’ scenario, both partners are working towards not just preserving, but increasing shareholders’ value in any business operation.

Prepare for the 2010 CGEIT Exams

ORDER NOW—2010 CGEIT Review Materials for Exam Preparation and Professional Development

To pass the Certified in the Governance of Enterprise IT® (CGEIT®) exam, candidates should have an organized plan of study. To assist individuals with the development of a successful study plan, ISACA® offers several study aids and review courses (www.isaca.org/cgeitreview) to exam candidates.

CGEIT Review Manual 2010

The CGEIT Review Manual 2010 is a reference guide designed to assist individuals in preparing for the CGEIT exam and individuals wishing to understand the roles and responsibilities of someone with significant management, advisory or assurance responsibilities relating to the governance of IT. The manual has been developed and reviewed by subject matter experts actively involved in the governance of IT. This is the first edition of the manual.

This manual includes six chapters, each one devoted to one of the domains within the scope of the CGEIT job practice. Each chapter provides task and knowledge statements with supporting explanations and exhibits detailing their interrelationships. Sample practice questions and explanations of answers will assist candidates in understanding the topic areas. Also included are definitions of terms most commonly found on the exam and references for further study. The manual is a resource to those seeking global guidance and a strong understanding of effective approaches to the governance of IT.

The 2010 edition has been developed to help CGEIT candidates understand essential concepts and is organized to facilitate study in the following job practice areas:
- IT governance framework
- Strategic alignment
- Value delivery
- Risk management
- Resource management
- Performance measurement

To order CGEIT review materials for the December 2010 exam, visit the ISACA web site at www.isaca.org/cgetitbooks or see pages S1-S8 in this Journal.
Quiz #131

Based on volume 2, 2010—Security

Value—1 Hour of CISA/CISM/CGEIt/CRISC Continuing Professional Education (CPE) Credit

TRUE OR FALSE

SINGLETON ARTICLE
1. Logical access that is closer to data is generally considered more effective (provides more assurance) than those farther away. Thus, application access controls that are effective can possibly negate the risks associated with information security at the perimeter.

2. There is no need for IT auditors to segregate information security problems and risks from RMM (risk of material misstatement) in a financial audit. They are the same in the IT sophistication spectrum.

3. For those third-party providers whose impact is significant to the financial reports, the user auditor may choose to rely on a Statement on Auditing Standards No. 70 (SAS 70) audit (Type II) by the service auditor. Thus, the IT auditor may be asked to review the SAS 70 for effectiveness of IT controls over the service.

CLYDE ARTICLE
4. Cloud computing is an enabler for mobile computing, allowing applications to be used not only from traditional PCs and notebooks, but also from smartphones and handheld devices. It changes the security paradigm.

5. In the US, the Personal Data Privacy and Security Act of 2009 and the Data Breach Notification Act do not have bipartisan support and are unlikely to pass if they come to a vote.

6. Security professionals have to be more than just security experts. Now a sound business understanding is essential. Communication and collaboration skills are a must. New security professionals should work to become intimately familiar with the products and services their company offers.

SAYANA ARTICLE
7. Embedding intelligence into documents by itself cannot solve the information security issues. Even when documents and data stores have intelligence, they will need to recognize identities uniformly and consistently to be handled by the identities.

8. With a combination of facial feature recognition and voice and fingerprint matching, identifying and authenticating a person is now a proven solution, as these technology implementations have already reached high levels of reliability.

RAI AND CHUKWUMA ARTICLE
9. Awareness of the critical assets within an organization begins with an enterprise risk management (ERM) process. This process aligns the risks identified by the business to the IT environment.

10. For the past decade, experience has consistently shown that more than 80 percent of all security incidents occur within an organization. The majority of internal incidents are caused by a lack of knowledge of an organization’s policies and procedures.

11. There is a total reliance by some organizations on SAS 70 Type II reports for review of external vendors. While a SAS 70 report is good, it is not final. The IT auditor should first verify that there is a policy in place to address third-party connections.

PIRONTI ARTICLE
12. The goal of an information security and risk management (ISRM) strategy should be to complement business goals while maintaining a responsible level of risk management and security for the organization’s information infrastructure and data.

13. ISRM budgets are typically 5 percent of the overall IT budget without compliance activities and 15 percent when inclusive of compliance activities and non-IT requirements.

14. When developing an ISRM strategy, it is important to define the governance model and functional inventory of capabilities and services that will be provided by the organization. A modular format is preferable, allowing the organization to add, delete or modify functions as business conditions and requirements change.

15. The key features of an ISRM maturity level 4 include good/excellent efficiency, widely known and published status of control, and moderate associated residual risk.

16. Many organizations invest significant money and resources to obtain and maintain compliance to regulations and standards. A better approach often is to analyze the impact of not being compliant or to become only partially compliant.

SIVASUBRAMANIAN ARTICLE
17. Critical impact factors (CIFs) indicate what kind of damage the security incidents cause for the organization. CIFs can include those that are within the control of the organization and those that are not.

18. Steps for integrating the prioritized security requirements into the security management life cycle include tagging the assets with their impact factors. This is performed by the IT and business units together.
ISACA Journal
CPE Quiz
Based on volume 2, 2010—Security
Quiz #131 Answer Form

(Please print or type)

Name _____________________________________________

Address ____________________________________________

__________________________________________________

CISA, CISM or CGEIT# _________________________________

Quiz #131

True or False

RAI AND CHUKWUMA ARTICLE
9. __________
10. __________
11. __________

PIRONTI ARTICLE
12. __________
13. __________
14. __________
15. __________
16. __________

SAYANA ARTICLE
17. __________
18. __________

SIVASUBRAMANIAN ARTICLE
19. __________
20. __________

Call for Articles
for COBIT® Focus

The next issue accepting articles is October, volume 4, 2010.
Submission deadline is 10 September 2010.

Answers—Crossword by Myles Mellor
See page 49 for the puzzle.

Please confirm with other designation-granting professional bodies for their CPE qualification acceptance criteria. Quizzes may be submitted for grading only by current Journal subscribers. An electronic version of the quiz is available at www.isaca.org/cpequiz; it is graded online and is available to all interested parties.

If choosing to submit using this print copy, please e-mail, fax or mail your answers for grading. Return your answers and contact information by e-mail to info@isaca.org or by fax to +1.847.253.1443. If you prefer to mail your quiz, in the US, send your CPE Quiz along with a stamped, self-addressed envelope, to ISACA International Headquarters, 3701 Algonquin Rd., #1010, Rolling Meadows, IL 60008 USA.

Outside the US, ISACA will pay the postage to return your graded quiz. You need only to include an envelope with your address.

You will be responsible for submitting your credit hours at year-end for CPE credits.

A passing score of 75 percent will earn one hour of CISA, CISM or CGEIT CPE credit.
ISACA MEMBER AND CERTIFICATION HOLDER COMPLIANCE

The specialised nature of IT audit and assurance and the skills necessary to perform such audits require standards that apply specifically to IT audit and assurance. One of the goals of ISACA® is to advance globally applicable standards to meet its vision. The development and dissemination of the IT Audit and Assurance Standards are a cornerstone of the ISACA professional contribution to the audit and assurance community. The framework for the IT Audit and Assurance Standards provides multiple levels of guidance:

- **Standards** define mandatory requirements for IT audit and assurance.
- They inform:
  - IT audit and assurance professionals of the minimum level of acceptable performance required to meet the professional responsibilities set out in the ISACA Code of Professional Ethics
  - Management and other interested parties of the profession’s expectations concerning the work of practitioners
  - Holders of the Certified Information Systems Auditor™ (CISA®) designation of requirements. Failure to comply with these standards may result in an investigation into the CISA holder’s conduct by the ISACA Board of Directors or appropriate ISACA committee and, ultimately, in disciplinary action.

- **Guidelines** provide guidance in applying IT Audit and Assurance Standards. The IT audit and assurance professional should consider them in determining how to achieve implementation of the standards, use professional judgement in their application and be prepared to justify any departure. The objective of the IT Audit and Assurance Guidelines is to provide further information on how to comply with the IT Audit and Assurance Standards.

- **Tools and Techniques** provide examples of procedures an IT audit and assurance professional might follow in an audit engagement. The procedure documents provide information on how to meet the standards when performing IT auditing work, but do not set requirements. The objective of the IT Audit and Assurance Tools and Techniques is to provide further information on how to comply with the IT Audit and Assurance Standards.

COBIT® is an IT governance framework and supporting tool set that allows managers to bridge the gaps amongst control requirements, technical issues and business risks. COBIT enables clear policy development and good practice for IT control throughout enterprises. It emphasises regulatory compliance, helps enterprises increase the value attained from IT, enables alignment and simplifies implementation of the COBIT framework’s concepts. COBIT is intended for use by business and IT management as well as IT audit and assurance professionals; therefore, its usage enables the understanding of business objectives and communication of good practices and recommendations to be made around a commonly understood and well-respected framework. COBIT is available for download on the ISACA web site, www.isaca.org/cobit.

Links to current guidance are posted on the standards page, www.isaca.org/standards.

The titles of issued standards documents are:

- **IT Audit and Assurance Standards**
  - S16 E-commerce Effective 1 February 2008
  - S15 IT Controls Effective 1 February 2008
  - S13 Using the Work of Other Experts Effective 1 July 2006
  - S10 IT Governance Effective 1 September 2005
  - S9 Irregularities and Illegal Acts Effective 1 September 2005
  - S8 Follow-up Activities Effective 1 January 2005
  - S7 Reporting Effective 1 January 2005
  - S6 Performance of Audit Work Effective 1 January 2005
  - S5 Planning Effective 1 January 2005
  - S4 Professional Competence Effective 1 January 2005
  - S3 Professional Ethics and Standards Effective 1 January 2005
  - S2 Independence Effective 1 January 2005
  - S1 Audit Charter Effective 1 January 2005

- **IT Audit and Assurance Guidelines**
  - G32 Business Continuity Plan (BCP) Review From IT Perspective Effective 1 September 2005
  - G31 Privacy Effective 1 June 2005
  - G30 Competence Effective 1 June 2005
  - G29 Post-implementation Review Effective 1 January 2005
  - G28 Computer Forensics Effective 1 September 2004
  - G27 Mobile Computing Effective 1 September 2004
  - G26 Business Process Re-engineering (BPR) Project Reviews Effective 1 July 2004
  - G25 Review of Virtual Private Networks Effective 1 July 2004
  - G24 Internet Banking Effective 1 August 2003
  - G23 System Development Life Cycle (SDLC) Reviews Effective 1 August 2003
  - G22 Business-to-consumer (B2C) E-commerce Reviews Effective 1 October 2008
  - G21 Enterprise Resource Planning (ERP) Systems Review Effective 1 August 2003

- **Standards for Information System Control Professionals**

  - Effective 1 September 1999
  - P10 Business Application Change Control Effective 1 October 2005
  - P11 Electronic Funds Transfer (EFT) Effective 1 May 2007

  - 510 Statement of Scope
  - 520 Independence
  - 530 Professional Ethics and Standards
  - 540 Competence
  - 550 ISACA JOURNAL VOLUME 4, 2010

Standards, Guidelines, Tools and Techniques
## Leaders and Supporters

**Editor**  
Jane Seago

**Senior Editorial Manager**  
Jennifer Hajigeorgiou  
publication@isaca.org

**Contributing Editors**  
Sally Chan, CMA, ACIS, PAdmin  
Kamal Khan, CISA, CISSP, CITP, MBCS  
A Rafae, CISA, CGEIT, CIA, CQA, CFE, FCA  
Steven J. Ross, CISA, CBIP, CISSP  
Tommie Singleton, Ph.D., CISA, CMA, CPA, CITP  
B. Ganapathi Subramaniam, CISA, CIA, CISSP, SSCP, CCNA, CCESA, BS 7799 LA

**Advertising**  
The YGS Group  
advertising@isaca.org

**Media Relations**  
news@isaca.org

**Editorial Reviewers**  
Matt Altman, CISA, CISM, CGEIT  
Linda Betz  
Pascal A. Bizarro, CISA  
Jerome Capirossi, CISA  
Cassandra Chasnis, CISA  
Ashwin K Chaudhary, CISA, CISM, CGEIT  
Joao Coelho, CISA, CGEIT  
Reynaldo J de la Fuente, CISA, CISM, CGEIT  
Christos Dimitriadi, Ph.D., CISA, CISM  
Ken Doughty, CISA, CBCP  
Amuj Goel, Ph.D., CISA, CGEIT, CISSP  
Manish Gupta, CISA, CISM, CISSP  
Jeffrey Hare, CISA, CPA, CIA  
Francisco Iguaz, CISA, CGEIT, CISSP  
Romulo Lomparte, CISA, CGEIT  
Juan Macias  
David Earl Mills, CISA, CGEIT, MCSE  
Robert Moeller, CISA, CISSP, CPA, CSQE  
Aureo Monteiro Tavares Da Silva, CISM, CGEIT  
Gretchen Myers, CISSP  
Daniel Paula, CISA, CISSP, PMP  
Pak-Lok Poon, Ph.D., CISA, CSQA, MIEEE  
John Pouey, CISA, CISM, CIA  
Steve Primost, CISM  
Panvathi Ramas, CISA, CA  
David Ramirez  
Ron Roy, CISA, CRP  
Johannes Tekle, CISA, CIA, CFS  
Ellis Wong, CISA, CFE, CISSP

**ISACA Board of Directors (2010-2011):**

- **International President**  
  Emil G. D’Angelo, CISA, CISM  

- **Vice President**  
  Christos Dimitriadi, Ph.D., CISA, CISM

- **Vice President**  
  Ria T. Lucas, CISA, CGEIT

- **Vice President**  
  Hitoshi, Ota, CISA, CISM, CGEIT, CIA

- **Vice President**  
  Jose Angel Pena Ibarra, CGEIT

- **Vice President**  
  Robert E. Stroud, CGEIT

- **Vice President**  
  Kenneth L. Vander Wal, CISA, CPA

- **Vice President**  
  Rolf M. von Roessing, CISA, CISM, CGEIT

- **Past International President, 2007-2009**  
  Lynn Lawton, CISA, FBCS CITP, FCA, FIIA

- **Past International President, 2005-2007**  
  Everett C. Johnson Jr., CPA

- **Director**  
  Greg Grocholski, CISA

- **Director**  
  Tony Hayes

- **Director**  
  Howard Nicholson, CISA, CGEIT

- **Chief Executive Officer**  
  Susan M. Caldwell

---

**ISACA Journal**, formerly Information Systems Control Journal, is published by ISACA, a nonprofit organization created for the public in 1969. Membership in the association, a voluntary organization serving IT governance professionals, entitles one to receive an annual subscription to the ISACA Journal.

Opinions expressed in the ISACA Journal represent the views of the authors and advertisers. They may differ from policies and official statements of ISACA and/or the IT Governance Institute and their committees, and from opinions endorsed by authors, employers or the editors of this Journal. ISACA Journal does not attest to the originality of authors’ content.

© 2010 ISACA. All rights reserved.

Instructors are permitted to photocopy isolated articles for noncommercial classroom use without fee. For other copying, reprint or republication, permission must be obtained in writing from the association. Where necessary, permission is granted by the copyright owners for those registered with the Copyright Clearance Center (CCC), 27 Congress St., Salem, Mass. 01970, to photocopy articles owned by ISACA, for a flat fee of US $2.50 per article plus 25¢ per page. Send payment to the CCC stating the ISSN (1526-7407), date, volume, and first and last page number of each article. Copying for other than personal use or internal reference, or of articles or columns not owned by the association without express permission of the association or the copyright owner is expressly prohibited.

Subscription Rates:

- **US:** one year (6 issues) $75.00
- **All international orders:** one year (6 issues) $90.00. Remittance must be made in US funds.

ISSN 1944-1967

---

### Advertisers/Web Sites

<table>
<thead>
<tr>
<th>Company</th>
<th>Website</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Audit 2 Ltd.</td>
<td><a href="http://www.audit2.com">www.audit2.com</a></td>
<td></td>
</tr>
<tr>
<td>CCH Teammate</td>
<td><a href="http://www.CCHGroup.com/ISC">www.CCHGroup.com/ISC</a></td>
<td></td>
</tr>
<tr>
<td>ExamMatrix</td>
<td><a href="http://www.ExamMatrix.com/ISJ">www.ExamMatrix.com/ISJ</a></td>
<td>15</td>
</tr>
<tr>
<td>ISACA San Francisco Chapter</td>
<td><a href="http://www.fs/isa.com">www.fs/isa.com</a></td>
<td>48</td>
</tr>
<tr>
<td>Modulo Technology</td>
<td><a href="http://www.modulo.com">www.modulo.com</a></td>
<td>1</td>
</tr>
<tr>
<td>Regis University</td>
<td><a href="http://www.RegisDegrees.com">www.RegisDegrees.com</a></td>
<td>6</td>
</tr>
<tr>
<td>University of Maryland University College</td>
<td><a href="http://www.umuc.edu/cyberedge">www.umuc.edu/cyberedge</a></td>
<td>9</td>
</tr>
<tr>
<td>Visual Click</td>
<td><a href="http://www.visualclick.com">www.visualclick.com</a></td>
<td>3</td>
</tr>
</tbody>
</table>