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 "silod" 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.
The ISACA® Journal seeks to enhance the proficiency and competitive advantage of its international readership by providing managerial and technical guidance from experienced global authors. The Journal’s noncommercial, peer-reviewed articles focus on topics critical to professionals involved in IT audit, governance, security and assurance.

Columns

4
IS Security Matters: Recovery in the Cloud
Steven J. Ross, CISA, MBCP, CISSP

6
IT Audit Basics: IT Audits of Cloud and SaaS
Tommie W. Singleton, Ph.D., CISA, CITP, CMA, CPA

9
Five Questions With...
Charan Kumar, CISA, CEGIT, CIA, CFE, FCA

Features

12

17
Book Review: Security, Audit and Control Features Oracle® Database, 3rd Edition
Reviewed by K. K. Mookhey, CISA, CISM, CISSP

18
Business Skills for the IT Audit and Assurance Professional
Robert G. Parker, CA+CISA, CMC, FCA

26
Building Your Bridge to the Future
James Reed, FCIPD

31
Information Security Career Planning: Education, Training and the Role of Professional Certifications
Kenneth Newman, CISM, PMP, ITIL/ITSM

35
Audit Careers 2010: The Swing of the Pendulum
Richard Tuck, CES, CPC, CIPC

40
It’s Not Easy Being Green: How the Green IT Movement Is Impacting Careers in IT Audit
Michael Juergens, CISA, CEGIT

43
The Social Psychology of IT Security Auditing From the Auditee’s Vantage Point: Avoiding Cognitive Dissonance
Thomas J. Bell III, Ph.D., CISA

48
IT Risk Analysis—The Missing “A”
Eric J. Brown and William A. Yarbary Jr., CISA, CPA

Plus

53
Crossword Puzzle
Myles Mellor

55
Help Source Q&A
Gan Subramaniam, CISA, CISM, CIA, CISSP, SSCP, CCNA, CCSA, ISO 27001 LA

57
CPE Quiz #130
Based on Volume 1, 2010
Prepared by Kamal Khan, CISA, CISSP, CITP, MBCS

59
Standards, Guidelines, Tools and Techniques: ISACA Member and Certification Holder Compliance

S1-S4
ISACA Bookstore
Price List Supplement

Journal Online

Want more of the practical, peer-reviewed articles you have come to expect from the Journal? Additional online-only articles will be available on the first business day of each month in which no Journal is released, i.e., February, April, June, August, October and December. These articles will be available exclusively to ISACA® members for their first year of release. Use your unique member login credentials to access them at www.isaca.org/journalonline.

Online Features

The following articles will be available to ISACA members online on 1 June 2010.

Book Review: IT Outsourcing Part 1: Contracting the Partner—A Management Guide
Reviewed by Gail Michaelson, CISA, PMP, SSGB

Making Sure You Really Are Walking on Cloud Nine
Tanak Modi, CISSP, PMP

Tackling Cybercrime: Divide and Conquer
Henk-Jan van der Molen

Please fill out the reader survey at www.isaca.org/readersurvey to help us improve the Journal to better serve our readers.
At SecureWorks, we turn raw security data into actionable security information. With the massive volume of relevant incidents we collect and analyze every day, we are able to better understand the threat landscape across the globe. We use that information to identify threats sooner and better protect our clients. Of our largest competitors offering security services, we’re the only ones focused exclusively on security. Discover what makes us different, and learn how our information can help keep yours safer.

See what the leading analysts say at secureworks.com/focused

Contact SecureWorks at info@secureworks.com or call 877.905.6661.

©2010 SecureWorks. All rights reserved. SecureWorks and the SecureWorks logo are registered trademarks of SecureWorks.
Recovery in the Cloud

In a previous column, I wrote about information security in the age of cloud computing.\textsuperscript{1} That era, of course, is still in the future, but if present trends continue, the Age of Cloud Computing will soon be upon us. Any organization planning to utilize cloud computing services should be well aware of the risks and should implement a robust control structure to counter them. Among the foremost risks is disruption of service, which includes both downtime and data loss.

**PROMISE AND CONCERN**

There are aspects of cloud computing that raise concern, and others that promise significant recoverability. Cloud computing is a set of utility services backed by a virtualized infrastructure that is highly scalable in response to the ebb and flow of business demands. It is geographically dispersed, designed for user self-service and (most important for a discussion of recoverability) self-healing.\textsuperscript{2} The internal structure of cloud computing is based on architecture in which services are offered from multiple physical data centers—all of this masked from the end user. Data are routinely replicated from site to site, so that if one location is disrupted, damaged or destroyed, one or more of the others can continue processing.

Virtualization is the basis for recovery. A vendor can rapidly re-create an entire processing environment by porting the virtualized image from one location to another, including the server(s), storage and network interface.

**IF IT WORKS**

This seems like all promise, no risk; the concern derives from a single, significant caveat: *if it works*. And sometimes, it does not work. A few recent examples demonstrate the potential fragility of cloud computing:

- In October 2009, the telecommunications carrier T-Mobile lost the data it was storing for users of Microsoft’s Sidekick system. Although a solution was eventually developed, some individuals lost their contact lists, calendars, notes, tasks, photographs, etc.\textsuperscript{3}
- In December 2009, Amazon’s EC2 cloud services were disrupted for six hours by a power failure in their Virginia, USA, data center. Due to connectivity issues, the redundancy protection designed into Amazon’s system failed to utilize unaffected data centers.\textsuperscript{4, 5}
- Workday, a small Software as a Service (SaaS) provider, suffered a 15-hour outage in September 2009, which was ironically caused by the backup to a system with built-in redundancy that took itself offline.\textsuperscript{6}

In a sense, it is unfair to highlight the failures of cloud computing services, inasmuch as organizations’ internal computing systems are no less vulnerable to failure than those of service providers. The fact that specific cloud computing failures are newsworthy does point out the relative rarity of outages, even (perhaps particularly) at this early stage of the technology. Fair or unfair, it is a concern that every acquirer of cloud computing services should be cognizant of and responsive to. Specifications of meantime to failure, meantime to repair and service level agreements should be part of every contract with a cloud computing provider. And, every customer should have some independent, audited assurance that the services acquired are resilient or at least readily recoverable within defined time frames.

**AUDITING CLOUD COMPUTING RECOVERABILITY**

Of course, gaining that assurance is not a simple matter. A customer might try to include a right to audit into a contract, but this is difficult to obtain. If audits were possible, it would then fall to that company’s internal auditors to determine that the terms of the contract are met, which again would be quite challenging from an outside viewpoint. Third-party audits are another solution, with the proviso that the scope and objectives of such an audit explicitly include recoverability. This is often not the case,\textsuperscript{7} and so the terms of a third-party audit should be carefully scrutinized. Frankly,
I am not aware of any cloud computing vendor that offers a third-party audit report of its recoverability practices. I would welcome learning of vendors who do so.

No such audit can offer assurance that a computing service would never fail, nor can it offer assurance of the amount of recovery time if a failure does occur. But, certain assertions are auditable: the number and frequency of recovery tests, the time interval for replication among sites, the existence of a disaster recovery plan with specified roles for emergencies, the training of staff in their emergency roles, and so on. It would be valuable to have assurance that a cloud computing vendor could use its data centers to reinforce one another. Do the data centers each have sufficient (i.e., excess) capacity? Are they far enough from one another that an incident affecting one will not also disable the other(s)? Contrariwise, if instantaneous recovery with no data loss is a customer requirement, are the data centers close enough to each other to make this possible?

Auditors should note that the questions to be answered in an examination of a cloud computing vendor are the same as those for internal recovery capabilities. The audit challenges are the same as those for outsourcing, which is an attribute of cloud computing, but not its definition. The core of the cloud computing promise is that the use of computing services is distinct from the ownership and operation of equipment and facilities.

RaaS

Use of the cloud as an alternative to recovery data centers is an intriguing but relatively little-explored possibility. I refer to it as RaaS, recovery as a service. A customer would acquire storage as a service to back up all or part of its data. In normal times, only one application would run, constantly updating the virtualized database, either through straightforward replication or by applying log files. If ever the customer’s primary data center were incapacitated, its applications, infrastructure and network would be inflated in the cloud to continue operations while the primary site was being recovered or repaired. Such an arrangement would provide exceptional flexibility for customers and reduce the level of effort of disaster recovery testing. In fact, an organization could run recovery tests as often as it would like, from the comfort of a tester’s office.

The economics of RaaS are not sufficiently advanced to make this a routinely adopted service. The cost of storage, even in virtualized form, is an inhibitor, as is the expense of software and network capacity to replicate databases. These strike me as obstacles that will be overcome as the service, and cloud computing as a whole, matures.

I believe that recoverability as such is not a central problem of cloud computing; recoverability is intrinsic to the architecture of the cloud. Reliability is the real challenge, changing if it works to it works. Reliability is a matter of confidence, which in turn comes from experience. In time, we will consider the cloud as reliable as, say, a company’s centralized computers. This may not be very reassuring, but we have learned to survive with that level of reliability in our data centers. The cloud may be much better...when it works.

ENDNOTES

1 “Cloudy Daze,” ISACA Journal, ISACA, USA, vol. 1, 2010
4 Thibodeau, Patrick; “Amazon’s Data Center Outage Reads Like a Thriller,” Computerworld, 11 December 2009, www.computerworld.com/s/article/9142154/Amazon_s_data_center_outage_reads_like_a_thriller
7 I have tried to avoid references to specific audit standards, which differ from country to country. In the US, a Service Auditor Report (SAS 70) or, in Canada, a CICA 5970 report, generally excludes recoverability from the scope of a system of internal controls. Readers should consult the auditing standards in each country as appropriate. Overall, it would be best to obtain an audit specifically focused on recovery capabilities.
8 Some vendors do tout their recoverability capabilities, and some are even offering recovery services such as I describe here. But, these are very recent announcements and raise as many questions as they answer.
IT Audits of Cloud and SaaS

Moore’s Law has been operating for decades without signs of slowing down, which leads to new technologies and, thus, new challenges for IT auditors. In recent months, cloud computing and Software as a Service (SaaS) have led the “bleeding edge” of IT. Therefore, IT auditors need to understand these technologies, establish an approach for identifying the key risks and develop effectual audits of the technologies for those risks. However, the risk-based approach (RBA) process for cloud computing is complicated by the fact that all of the technologies and controls are housed outside the entity being audited.¹ ² ³

A key to IT audits of cloud computing and SaaS is to choose a framework for the components that assists an effective risk assessment of those technologies. Once a proper risk assessment is produced, the IT audit becomes a natural extension of auditing for the identified risks, especially where controls have not adequately mitigated the risk. This RBA is the common approach for audits of various types today.

COMPONENTS OF CLOUD COMPUTING

Much has been written about cloud computing, SaaS and data centers, but often those technologies are melded as a composite service referred to as cloud computing. Actually, there is a simple framework for thinking about cloud computing that should help IT auditors in performing a risk assessment. The components are Infrastructure as a Service (IaaS) and Software as a Service (SaaS)—almost identical to the way we think of the body of technologies internal to an entity.

CLOUD COMPUTING: IaaS

Services of IaaS components replace or supplement the internal infrastructure. The key decision factors for management in deciding to move to IaaS (outsourcing part of its infrastructure) and choosing the appropriate vendor are usually efficiency-related. For instance, it takes one full-time employee (FTE) “blank amount of time” per year to manage about 70 servers. If the entity has a server farm, it can outsource those costs to an effective data center and reduce costs significantly. In addition, when the entity needs to upgrade its software, or acquire a new software application, the consideration of infrastructure is probably an insignificant consideration regarding cost, assuming the choice in IaaS provider was sufficiently sophisticated, and requires little to no changes to its own infrastructure.

There is also the accounting consideration. Usually, infrastructure costs are substantial and, according to the Generally Accepted Accounting Principles (GAAP), are treated as a capital expense (CAPEX). However, if the infrastructure is outsourced, the expense associated with the IaaS infrastructure usually becomes an operating expense (OPEX). In the US, this leads to a tax advantage regarding income taxes.

Thus, some of the key factors for management when choosing the IaaS provider are flexible performance (including scalability) and availability while achieving physical and virtual security needs.

There are various ways to break down IaaS, but here is one way:

• Connectivity
• Network services and management
• Compute services and management
• Data storage
• Security

Connectivity obviously refers to reliable access to the Internet and connectivity to associated systems and technologies, for instance, data storage to application servers. Examples of risks would be availability/downtime and speed of access.⁴ The average entity experiences one day per annum of downtime.

Network services and management includes not only providing network capabilities, but managing the network, monitoring the network and providing for efficient access through aspects such as load balancing. Examples of these risks...
are scalability for new technologies or expanding the level of transactions, availability, secured transmissions, and the level of access (e.g., load balancing).

Compute services and management include appropriate resources such as core, processors, memory and managing the operating system (OS). Examples of the risks are availability (including system failure) and scalability.

There has been significant growth in data centers over the last few years, and data centers are becoming more sophisticated in the scope of services. Examples of the risks for data storage include the obvious: security of data, recovery, availability and scalability. The security and recovery issues are particularly important. Management should ensure that the data storage aspect of IaaS can provide an appropriate level of physical and logical security and an appropriate recovery methodology to ensure a timely recovery if the data center is involved in a disaster.

Security issues are more or less ubiquitous for IaaS and include physical security, especially data storage, and logical security. They include security from unauthorized access by malicious intruders and rogue employees of the IaaS provider. In fact, the latter is an increased risk to the user entity that needs to be addressed via adequate controls by the service entity.

Risks are always determined within contextual circumstances to the entity—for example, the industry, its own business processes, the current economy and other circumstances peculiar to the entity at that time. Some of the other issues that may be risks are ownership, insurance, project management and performance reporting.

Mitigating controls could be discoverable from a SAS 70 Type II audit report. If one exists for the IaaS provider, the IT auditor should certainly read it to see what level of assurance can be gained for the specific, identified risks. Controls the provider should be employing include best practices in security, support (e.g., IT Infrastructure Library [ITIL] v3) and business recovery.

**Cloud Computing: SaaS**

Some of the key points in deciding to use SaaS, or a particular vendor, are the complexity of the environment, the need to buy smaller pieces/modules, compatibility with existing systems and IT (including programming platform), ease of purchase, ease of integration, project management, scalable infrastructure, and billing/costs (metering).

There are various ways to break down SaaS, but here is one framework:

- Business process modeling
- Evaluation and analysis
- Process execution

Business process modeling involves the need to fit together workflow/business process structure, applications and data, organizational structure, and the integration of existing systems. Evaluation and analysis includes process cost accounting, balanced scorecards, service level agreements (SLA), process warehouse and optimization. Process execution includes workflow control, applications integration (enterprise application integration [EAI]), service orchestration (service-oriented architecture [SOA]), populating databases/conversion and business activity monitoring. Other issues include document and content management, collaboration, systems management and administration, and various aspects of management of SaaS.

Examples of risks would be related to these areas. Some examples include an improper fit of the business process to the application, inadequate connectivity between applications and data, improper integration with existing systems, and inadequate monitoring of SaaS business processes and events. Obviously, the SLA is a key audit objective. There is also a risk of cost control and estimates; that is, it is possible that the move could end up costing the entity more rather than less. One example of cost control is the metering/billing aspect of SaaS, which presents an area of potential risk.

**IT Assurance Framework**

ISACA’s IT Assurance FrameworkTM (ITAF™) includes a section (3630.6) on outsourcing and third-party activities (see figure 1). Cross-references are included—ConT™ PO4, PO7, PO8, PO9, AI2 and AI5, and ISACA IT Audit and Assurance Guidelines (formerly IS Audit Guidelines) G4, G18, G32 and G37. These referenced documents provide useful technical assistance in conducting an IT audit for cloud computing.

Obviously, the fact that a third party is involved means direct auditing of the service entity may not be practical or
even possible. ITAF also supplies a list of potential documents that could provide service audit information that should be relevant (see figure 2).

CONCLUSION
Auditing cloud computing in one sense is like auditing any new IT—understand the IT, identify the risks, evaluate mitigating controls and audit the risky objects. The understanding and risk assessment can be enhanced with a good framework to think about the IT and risks and, thus, assist the IT auditor in conducting an effectual risk assessment. The IaaS/SaaS framework described here is intended to assist IT auditors in performing their duties associated with cloud computing.

Figure 1—Types of Reports Based on User Needs

| 3630.6 Outsourced and Third-party IT Activities | • G4 Outsourcing of IS Activities to Other Organisations  
• G18 IT Governance  
• G32 Business Continuity Plan (BCP) Review From an IT Perspective  
• G37 Configuration Management Process  
• ConIT:  
– PO4 Define the IT processes, organization and relationships  
– PO7 Manage IT human resources  
– PO8 Manage quality  
– PO9 Assess and manage IT risks  
– AI2 Acquire and maintain application software  
– AI5 Procure IT resources. |
| Consulting Services | Attestation Procedures | Agreed-upon Procedures | SAS 703 S-59704 | TrustServices SysTrust and WebTrust |
| A report that provides: | No assurance | Assurance | No assurance | Assurance | Assurance based on predefined criteria |
| A report that will be available for: | Restricted use to a predefined audience | General distribution | Restricted use to those who have agreed to the procedures | Restricted use to current customers and their auditors | General distribution |
| A report that will disclose: | Detailed information | Limited information | Specific procedures and factual findings | Detailed information | Specific information that may be in summary or detailed form |


Figure 2—ITAF Guidelines for Audits of Third-party IT Activities

| A report that provides: | No assurance | Assurance | No assurance | Assurance | Assurance based on predefined criteria |
| A report that will be available for: | Restricted use to a predefined audience | General distribution | Restricted use to those who have agreed to the procedures | Restricted use to current customers and their auditors | General distribution |
| A report that will disclose: | Detailed information | Limited information | Specific procedures and factual findings | Detailed information | Specific information that may be in summary or detailed form |


ENDNOTES
2 Ross, Steve; “Cloudy Daze,” ISACA Journal, ISACA, USA, vol. 1, 2010
4 Each IT audit has its own context (e.g., financial audit, internal audit, special IT audit). Each IT audit has its basic objectives. Thus, the scoping aspects of a particular IT audit would review all of these risks for various aspects of cloud computing and determine whether they are applicable and relevant.
Charan Kumar began his career in programming in various roles, including systems analysis, design and development. Appreciating the need for an in-depth understanding of business operations by IT professionals, Kumar pursued the Chartered Accountant certification. While in the CA program he experienced firsthand the increased reliance of organizations on information technology and foresaw the changing role of financial audit, with information systems (IS) audit as an area of expertise. He then earned his Certified Information Systems Auditor™ (CISA®) designation. Based on various cases investigated by Kumar, he was conferred the Certified Fraud Examiner designation in 1996. Subsequently, he earned the Certified Internal Auditor (CIA) and Certified in the Governance of Enterprise IT® (CGEIT®).

With the intent to increase the awareness of ISACA in India, he—together with his colleagues at the New Delhi Chapter—organized the first ISACA international event in India in 1996. This event in New Delhi was succeeded by the formal launch of the Mumbai Chapter, and many other chapters in India were soon to follow. Kumar was instrumental in the formation of the New Delhi Chapter of ISACA of which he is the founding president.

Kumar spent 18-plus years in the profession, at Coopers & Lybrand, Ernst & Young and KPMG, among others, and more than five years in the industry with a leading shipping line in the Middle East. He regularly speaks at various conferences and has served on ISACA’s Education Board and various program committees. He currently serves on the ISACA Toronto Chapter’s Research and Academic Relations Committee.

Outside of his career and association with various organizations, Kumar enjoys the outdoors and trekking. When away from work, he can be spotted flying a Cessna through the eastern Toronto skies. He can be reached at ckumar@femhillassociates.com.

Q What do you see as the biggest risks being addressed by IS auditors? How can businesses protect themselves?

A An organization’s ability to understand IS/IT risks influences its initiative to mitigate them. Given the complexity and pace of change in technology, IS/IT risks and exposures are constantly evolving. There is always a large risk that leadership within business may not be able to comprehend the urgency and complexity of IS/IT risks. IS auditors address this risk via their audits and reports by bringing to the business leadership’s attention the IS/IT risks, as well as recommendations to mitigate them.

Businesses can shield themselves by recruiting resources with the appropriate blend of skills within their team, for example, CISA- or CISM-certified auditors. The collective skill set supports a quality audit, and management can expect a fair degree of assurance that IS/IT risks are identified and appropriate risk mitigation recommendations are made.

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 paths and look at the future of IT auditing?

A In essence, the role has not changed much over the past many decades. That is, IT auditors are still identifying IS/IT risks and providing recommendations to mitigate them. What has changed is the IS/IT knowledge domain.

An auditor’s understanding of the role of technology in business is very important. This can assist in appreciating IS/IT risks from a business perspective, i.e., identifying the impact of each risk by responding to the “so what?” question for every risk identified. This can also help in articulating the business impact of IS/IT risks and can contribute to the “value add” while also facilitating buy-in from senior leadership.
Q How do you believe the certifications you've attained have advanced or enhanced your career? What certifications do you look for when hiring new members of your team?

A Absolutely, they have had a tremendous positive influence. CISA was my first. Certification is granted by a professional institution when a candidate demonstrates adequate understanding of the subject via the exams, and obtains minimum practical experience. Certifications provide assurance that a candidate has the minimum professional expertise expected in the field. This opens doors as employers or clients know what to expect.

When hiring, CISA of course is the minimum for IT auditors. As auditors, we constantly face challenges; hence, the attitude of the candidate is very important. If potential candidates do not have the CISA certification, I typically encourage them to work toward their designation, and I provide the required support to help them accomplish this.

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

A There is increased awareness and appreciation of IT governance compared to a few years ago. I expect organizations that have implemented IT governance and best practices to realize economic benefit due to their adoption. As a result, this economic success will likely stimulate further industrywide acceptance of IT governance.

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

A Auditors are seen, more often than not, in a policing role. This makes the auditee very defensive, challenging findings and resisting recommendations.

I have found upfront articulation of expectations and categorical expression of an auditor’s role to clients very helpful. It is also important for auditors to demonstrate objectivity and fairness in attitude and appearance in their dealings with clients. This brings significant respect for auditors. They are then seen as doctors who diagnose the patient, identify problems and prescribe recommendations that may not always contain “good news.” At the same time, the patient appreciates the value-add provided by the doctor.
YOUR SUPPORT TEAM’S SILVER BULLET.

QUICK ON THE DRAW AND QUICK TO SOLVE!

A legendary support team is already in your office — they just need the right tool. GoToAssist connects your team with your customers like never before with simple, powerful remote support.
Numerous Opinions—Which Will Happen?  
A Review of 2010 IT Trends and Predictions

The trends noted here were compiled at the request of ISACA’s Strategy Advisory Council. After reviewing the document, the council believed that such a compilation would be of value to ISACA members and Journal readers. The compilation was summarized to fit within the pages of the Journal. Please see the references for more details.

Get 20 experts in a room and ask them to prognosticate, and you will get 30 opinions. This seems to be the case with this year’s group of IT trend spotters. While there is a difference of opinion in some areas (e.g., IT spending), there are a few topics that seem to be widely accepted as taking center stage in 2010.

The following sections summarize the findings of a number of the major IT trend spotters.

IT EMPLOYMENT PREDICTIONS FOR 2010
Foote Partners’ offers the following IT employment predictions for 2010:

1. **IT unemployment overall has stabilized and steady momentum in services sector job gains has been offset by continued volatility elsewhere.** Five IT bellwether job segments reported in the US Department of Labor statistics lost 7,300 jobs in September, October and November 2009 but added 18,500 jobs for a net gain of 11,200 jobs. By contrast, for the first eight months of 2009, the same five IT job segments experienced a net loss of nearly 31,000 jobs.

   The most robust job segment, Management and Technical Consulting Services, gained a net 13,600 jobs in the first 11 months of 2009. A second segment in the same job category, Computer Systems Design and Related Services, posted a net loss of 7,800 jobs in the same 11-month period, but a gain of 5,500 jobs in October and November. Not so lucky in 2009 were services jobs, as the Data Processing, Hosting, and Related Services segment showed a net loss of 6,700 jobs since the start of 2009.

2. **Slim to no chance for meaningful IT jobs recovery in 2010.** IT hiring overall will not pick up noticeably until late in 2010, and more likely 2011. Volatility will continue to punctuate staffing and pay levels throughout 2010, with human capital investments focused on specific IT skill specializations as employers struggle to recalibrate their IT workforces by striking the right balance among costs, agility and intense competitive market pressures.

3. **Investments focus more on skills than jobs in 2010.** As throughout 2009, the emphasis is less on jobs and hiring and much more on filling critical skills needs…acquired from the inside (hiring, training), from the outside (contractors, consultants), “rented” via outsourcing and offshoring, or “given over” by purchasing any number of managed services. Hiring restrictions, combined with business leaders demanding quicker, high-impact, predictable, cost-effective execution, will continue in 2010 to refocus employers on skills, not jobs. …The biggest downside of this skills focus and accelerated process: Quick decisions to cast off anybody and anything that is a drag on finite resources often result in unfortunate consequences post-recession when unique experience and skills held by certain cast-offs are desired once again.

4. **IT services employment sector is first to recover, but differently for small vs. large vendors.** The search will be even more frantic next year for right-skilled IT contractors, consultants and even managed services that can be depended on to perform critical work—a boon for the IT services sector. Boutique small and medium-sized business (SMB) consulting firms in hot segments such as security will continue to experience acute talent shortages against a steady drumbeat of demand for their specialized services, which are generally regarded very highly for their quality, reliability, relationship management and competitive pricing (vs. their much larger competition).

5. **For short- (and long-) range IT job security, the smartest place to be in 2010 is IT security.** Unlike other technology job segments, pay and demand for security skills have risen steadily since 2007, and neither budget nor headcount...
has diminished in economic hard times. Driving continued momentum for steady jobs investment and career safety are more regulation; constant fear of increasing threats; greater customer expectations and demands aimed at vendors; and the splitting of business/strategic risk and operational security activities, which has been accelerated by market forces. Also in demand: SAP professionals; IT specialists who can engage audiences in their company’s messages, products and services via social media; web development; e-commerce applications and systems; and business intelligence skills and competencies.

6. **The X factor: managed services adoption.** Impressive growth projections for the next three years—compound annual revenue growth estimates in the 10 percent to 39 percent range are common for several service segments—portend the beginning in 2010 of widespread IT workforce reconstitution, allowing employers to start to properly synchronize on-board skill sets with rapid-change business requirements. The goal is lean, nimble, reactive and predictable human capital deployment with less waste.

**IT SPENDING IN 2010**

Gartner concluded that the economic crisis has irrevocably changed the business oversight of IT investments. The tighter linkage established during 2009 between IT spending and business performance metrics is here to stay.²

According to a Forrester survey³ of more than 900 IT executives and technology decision makers in Canada, France, Germany, the UK and the US, IT contractors and consultants will see the deepest decreases in spending for their services, while systems integration and outsourcing services will have the greatest increases. Unlike the last recession from 2001 to 2002 when outsourcing and offshoring experienced growth from firms seeking to reduce internal IT costs, the spending picture for IT services this time around is much more mixed.

When asked about changes they expect to see in their organization’s total spending on IT services:

- 50 percent said they plan to increase spending on systems integration and project work
- 26 percent plan increases in applications outsourcing
- 25 percent expect to increase spending on infrastructure outsourcing
- 41 percent expect to reduce spending on contractors
- 34 percent foresee lower spending on IT consulting

In a poll of 594 IT leaders, the annual 2010 State of the CIO Survey⁴ found that about two-thirds of CIOs, or 62 percent, have canceled or postponed projects during the past year as a result of unfavorable economic conditions. The projects on which they have focused are those that can enhance their company’s products and spur sales.

The “Five Infrastructure Trends to Watch for in 2010,” in CIO Update found that enterprise IT organizations will have no options but to reduce their IT spending. 2009-10 will see a significant drop in the IT operations budget. Upgrades, new technology adaptations and new tool implementations will be curtailed, deferred or canceled. Support agreements with product vendors and service providers will be renegotiated and IT will move to efficient “lights on” operations.³

The CIO Update article agreed with the State of the CIO Survey findings, noting that “projects that have short- and medium-term savings potential will gain acceptance.”⁶

**IT TRANSFORMATION DURING ECONOMIC RECOVERY**

The IDC Predictions team⁷ predicted that 2010 will be a year of modest recovery for the IT and telecommunications industries. Other industries will come out of the recession with a transformation agenda and will look to IT as an increasingly important lever for these initiatives.

The recovery, according to IDC, will not mean a return to the prerecession status quo, but rather, will result in a radically transforming marketplace, driven by surging demand in emerging markets, growing impact from the cloud services model, an explosion of mobile devices and applications, and the continuing rollout of higher-speed networks. IDC anticipates 3.2 percent growth for 2010, returning the IT industry to 2008 spending levels of about US $1.5 trillion.

The CIO Update article noted the following relevant trends:

- Processes implementation will increase across IT to improve efficiency and reduce dependence on people. Dependence on people in IT is increasingly affecting productivity and efficiency.
- Service level agreement (SLA)-based managed services will take over from staff augmentation. Managed services will relieve IT managers from day-to-day management of certain operation tasks. As managed services gain momentum this year, customer and end user satisfaction will come to the forefront as SLAs will be tied to customer satisfaction.
• SMBs that traditionally resisted outsourcing will increasingly look at offshoring to reduce costs and increase efficiency. With environments becoming increasingly complex, and pressure mounting to reduce costs, the SMB segment is looking to offshore at least some of their IT infrastructure services or IT operations to save money.

• Remote production support is slowly picking up momentum as remote infrastructure management (RIM) providers are looking beyond infrastructure and have started providing production support and remote application support. The single service desk operations will help increase first call resolution.

Among the key findings of its “Top Predictions for IT Organizations and Users, 2010 and Beyond,” Gartner said that the balance of power in IT continues to shift toward external providers and users. It predicted that by 2012, 20 percent of businesses will own no IT assets.8

Among its trends for 2010, Verizon Business noted that businesses will make decisions in 2010 that will fuel their future growth. IP-based investments, such as unified communications, cloud computing and Software as a Service, will continue to provide the platform to enable successful business practices. In 2009, businesses learned how to do more with less. Applying 20/20 hindsight vision and lessons learned will inspire the 2010 technology decisions that will help businesses work harder and more efficiently for the next decade. In the process, businesses will work better and more effectively together to create a positive impact on the global economy and society.9

### 2010 Technologies Trends

As noted previously, 2010 will see a continuation of the trend toward a tighter link between IT spending and business performance. Therefore, there were many similarities in the technology trends for 2010:

• Cloud computing, and all aspects surrounding the cloud (e.g., standards, security)
• Making the workforce (more) mobile
• Green IT and issues of sustainability
• Social networking as a critical facet of the business landscape
• Growing need/desire for wireless “everything”

### References


Gammage, Brian; et al; “Top Predictions for IT Organizations and Users, 2010 and Beyond,” Gartner, 29 December 2009


ENdNOTES
2 Gammage, Brian; et al; “Top Predictions for IT Organizations and Users, 2010 and Beyond,” Gartner, 29 December 2009
6 Ibid.
8 Op cit, Gammage

Sharpen your skills and give yourself a major edge in the job market with a cybersecurity degree from University of Maryland University College (UMUC). Our degrees focus on technical and policy aspects, preparing you for leadership and management roles—and making you even more competitive for thousands of openings in the public and private sectors. Courses are available entirely online, so you can earn your degree while keeping your current job.

• Designated as a National Center of Academic Excellence in Information Assurance Education by the NSA and the DHS
• Advanced virtual security lab enables students to combat simulated cyber attacks
• Scholarships, loans and an interest-free monthly payment plan available

Enroll now. 800-888-UMUC • umuc.edu/cyberedge
On-site Training
What you need, where you want it, when you need it.

Tight budget? Busy schedule?
Multiple staff to train? No problem!
Save time and money—let ISACA®
bring the training to you.

www.isaca.org/onsitetraining2010
Oracle® is the most widely used database across the world. And even though databases hold some of the most sensitive information, they are often least understood in terms of security controls and auditing.

To address these gaps in an auditor’s understanding of Oracle and its security features, ISACA® offers the third edition of Security, Audit and Control Features Oracle Database. Although written from an auditor’s point of view, the book also serves as an excellent resource to the database administrator (DBA) looking to ensure compliance to security best practices. Chief information security officers (CISOs) and information security managers will also find value in the book as a source for a comprehensive set of database security controls.

The book begins by briefly discussing the history of the Oracle database and the security features gradually introduced from version 6 to the latest version 11g. It then describes important Oracle concepts, such as the difference between an instance and a database, the Oracle processes, and file structures. In chapters 5 and 6, the authors provide the basic background to planning the audit.

A secured database needs to run on a secured operating system. Oracle runs on a wide variety of operating systems, and in chapter 7, the authors cover important security controls for Windows and UNIX operating systems in which Oracle is installed.

In chapter 8, the authors cover the newer security features introduced in version 10g and 11g. Often, awareness of these features can push an organization to upgrade its current database versions.

In chapters 9 through 13, the authors cover key Oracle security features such as Oracle system privileges, controlling access to critical objects such as stored procedures and triggers, the use of roles to group users and permissions together, password controls, resource limits, database links and trusted relationships, operating system security, and network security controls.

Chapter 14 rounds up the discussion with information on general database security controls such as change management, segregation of duties, documentation, monitoring, vulnerability and patch management, and backup and recovery.

The huge dependence of organizations on applications and their underlying databases implies that the availability of the database often affects the very existence of a company. While the cost of an interruption depends on a number of factors, it can be significant enough to impact both the profitability and the reputation of any organization. In light of this, the book covers the important aspects of Oracle’s backup and recovery features, and its other disaster recovery and redundancy capabilities. The reader is encouraged to explore Oracle’s offerings such as Oracle Data Guard, Oracle Advanced Replication, Oracle Recovery Manager (RMAN) and Real Application Clusters (RAC).

The appendices present a wealth of useful information, including an introduction to automated Oracle security assessment tools, a comprehensive audit/assurance program and an internal control questionnaire (ICQ), recommendations for the professional, frequently asked questions, a glossary, an explanation of acronyms, and suggested readings. Appendix 4, Recommendations for the Professional, provides a 10-point list, including gems such as “befriend the DBA” and “think like a hacker.” This is a good example of the emphasis the book puts on the practical aspects of the subject at hand.

Overall, this book provides excellent coverage of Oracle security features and controls for the auditor, information security practitioner and the DBA preparing for their next database audit.

**EDITORS’ NOTE**

Security, Audit and Control Features Oracle® Database, 3rd Edition, 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.
A survey conducted in 2008 among audit committee members and auditors reporting to audit committees indicated that information technology, in itself, was not a key issue that audit committees could address. What was key was business, the uses business made of technology, the threats and risks associated with those uses, and the steps taken to mitigate those risks. The survey indicated that audit committees focused on business issues and treated technology as an enabler in business processes. A common theme was, “Do not tell me what controls are not effective; tell me what business process may be compromised, what business processes I cannot rely on, and their potential impacts if I do not address the risk.” In other words, the IT audit and assurance professional must become more business-focused.

That business focus may lead the IT audit and assurance professional into additional areas that encompass enterprise strategy, culture and goals, and the role that information technology plays in supporting these and other enterprise initiatives. Knowledge of business strategy, enterprise mission and goals, and monitoring objectives and key milestones, including effective measurement and benchmarking, may assist IT audit and assurance professionals in focusing their audit to better meet management’s and board of directors’ expectations.

Granted, the IT audit or IT review will focus primarily on technology issues. However, to be effective, IT audit and assurance professionals must report their observations and findings in business terms. In other words, they must write for their audience.

That may be easier said than done. IT audit and assurance professionals require deep technical knowledge to scope the assignment, conduct the assignment, assess the findings, and develop workable and effective recommendations in technology-complex environments.

IT audit and assurance professionals have attained certifications, such as the Certified Information Systems Auditor (CISA) and the Certified Information Security Manager (CISM), that demonstrate their knowledge and competence in IT audit and control as well as security management. These professionals are well recognized and appreciated for their technical knowledge and skill, but could they be more valuable to the enterprise?

The issue then becomes one of providing IT audit and assurance professionals with training in business—in other words, training that includes knowledge of key business processes, how businesses are organized, the environments in which they work, and the issues facing businesses in remaining compliant with an ever-increasing plethora of laws, regulations, rules, standards, industry guidelines and other requirements.

This article explores the rationale behind the drive to equip IT audit and assurance professionals with increased business skills and an increased understanding of the enterprise and how it operates. It addresses the pros and cons, as well as the issues that management, the general auditor, and the IT audit and assurance professional may raise. It presents a business case for expanding the business knowledge and role of the IT audit and assurance professional and how to get started with this business-oriented mind-set.

**ESTABLISHING GOALS**

Ultimately, IT audit and assurance professionals must be comfortable presenting technology-related business risks and their potential impacts to boards of directors, executive management and other stakeholders. Presenting technology issues in a business context ensures that management is better informed and better able to understand the risks, issues, implications and impacts when making technology-related business decisions.

Accordingly, IT audit and assurance professionals should have the skills to understand underlying business processes, which will enable them to convey their technical findings with a business focus.

Robert G. Parker, CA•CISA, CMC, FCA a retired Deloitte & Touche partner, is a past international president of ISACA and currently serves on the ISACA Frameworks Committee, the AICPA-CICA Privacy Task Force, the CICA Information Technology Assurance Committee and the Board of the University of Waterloo Centre for Information Systems Assurance. Parker is the primary architect of ISACA’s Information Technology Assurance Framework (ITAF). He is a frequent author and speaker on information security, control, risk management and privacy issues—areas in which he practices.
RELEVANT BUSINESS KNOWLEDGE

Business knowledge encompasses an understanding of businesses—what the business is—including legal status, organization, governance, structure, culture, risk tolerance or appetite, operations, and uses of technology in providing services to business units. Further, it includes what the business does, including products, services, markets, customers and users—in other words, an understanding of the business from the perspectives of different stakeholders.

It also includes knowledge of the business and industry environments, the governing laws and regulations, and the policies and procedures designed to encourage and enforce compliance. It involves an understanding of industry trends and best practices. It requires that the IT audit and assurance professional understand operational, financial, accounting and reporting systems and their uses within the enterprise. It also requires that the IT audit and assurance professional understand the business drivers and the business and industry risks that the enterprise must manage.

Figure 1 illustrates the interrelationship among the three fundamental components of business knowledge that are relevant to the IT audit and assurance professional: information technology, industry and business. These three components are influenced by, and, in some cases, operate in accordance with, the policies and procedures that establish an enterprise’s operating environment.

Knowledge and understanding of business information can help IT audit and assurance professionals better assess the impact of any identified risks and findings and communicate these in terms that are relevant and understandable to boards of directors, executives, senior and line management, and others who may not possess a detailed understanding of technology and its potential impact on the business. For example, there may be a lower tolerance for risk in publicly traded and/or highly regulated businesses than in privately held businesses. Accordingly, the IT audit and assurance professional’s business knowledge will assist them in developing relevant and practical recommendations that add value to the business.

IMPACT OF BUSINESS KNOWLEDGE ON AN IT AUDIT

Greater business knowledge will likely increase the relevance and practicality of IT audit findings and recommendations, in that they will address business impacts in terms that can be understood and assessed by management and others not possessing a detailed understanding of technology. Rather than indicate that a control is missing or is ineffective, the IT audit and assurance professional with appropriate business knowledge and skills should also identify the business impact, such as "shipping will not be possible" or "we may be in contravention of privacy laws," and quantify the risk in terms of the likely financial, reputational, legal or other impacts.

Improved findings and recommendations will increase the value of IT audit and assurance assignments to the business units, executive management and boards of directors by providing better and more effective decision-making information.

Audit committees tend to consider IT an integral component of business processes and deal with it as such. Accordingly, IT audit and assurance professionals possessing increased business knowledge will be able to discuss issues and impacts in terms that members of boards of directors can better comprehend and address.

Boards of directors need to understand the risks, mitigating initiatives being undertaken and any residual risks when dealing with core business processes. Further, when business strategy dictates changes, such as outsourcing, developing major systems or changing technologies, the IT audit and assurance professional will be better able to relate these in business, rather than technical, terms to the board of directors and senior management.
EIGHT BUSINESS KNOWLEDGE AREAS

Businesses maintain significant amounts of information that encompass business intelligence, knowledge of business processes, procedures and standards, knowledge of products and services, and information on markets and competition. With this wide range of information, the first task is to determine what business knowledge is relevant to IT audit and assurance professionals.

For ease of discussion, eight categories of business knowledge that IT audit and assurance professionals need to understand are defined:

- How is the enterprise organized?
- How is the enterprise governed?
- Under what laws/regulations does the enterprise operate?
- What are the enterprise’s business processes?
- How does the enterprise operate?
- How does the enterprise use technology?
- How does the enterprise finance itself?
- How does the enterprise measure business success?

The IT audit and assurance professional should understand the basic principles of business: planning, acquiring assets and other resources, producing goods or delivering services, evaluating performance, and determining how these principles relate to the business. In addition, there will likely be a need to acquire additional industry-specific knowledge, particularly in those industries in which procedures have become well recognized and adopted or are required by legislation, regulation, industry-adopted standards or legal agreement.

IT audit and assurance professionals should gain an understanding of the industry in which the enterprise operates. First, they should classify the enterprise into one of the 11 categories identified in figure 2. Industry knowledge serves to put organizational initiatives, changes, strategies and plans into context. It helps the IT audit and assurance professional comprehend the rationale for some of management’s decisions and the key external drivers.

While a wide range of knowledge is useful and may assist in the cross-pollination of ideas and techniques, IT audit and assurance professionals will likely focus on one or a limited number of industries in which they, their organization or clients are involved.

Accordingly, IT audit and assurance professionals would be responsible for understanding the regulatory environment only of their employers or, in the case of external audit and advisory professionals, the environments of their major industry focus.

Figure 2—Enterprise Classifications

- Financial services (e.g., banks, investment firms, insurance companies)
- Consumer-intensive (e.g., retail stores, direct marketing, service businesses, entertainment, hospitality)
- Health care (e.g., hospitals, health care providers, clinicians, technology providers, health insurance providers)
- Transportation (e.g., airlines, trucking, coastal and deep-sea shipping, railways)
- Government (e.g., federal, state/provincial, municipal and local, related boards and agencies)
- Resource industries (e.g., oil and gas, mining, forestry, exploration, extractions)
- Manufacturing (heavy and light industries)
- Extractive (e.g., energy, mining, agriculture, fishing)
- Utilities (e.g., hydroelectric, nuclear, coal generation, solar, wind turbines, tidal, gas distribution)
- Public sector (e.g., federal, subfederal and local government, public agencies and corporations, public education, military)
- Nonprofit organizations (e.g., associations, charities, foundations)

ORGANIZATION

The IT audit and assurance professional should understand the differences in the types of enterprises—how they are created, what legal authority they are given, and their reporting and filing obligations. This would involve gaining an understanding of the different forms of enterprises, such as limited liability companies, public vs. private companies, multijurisdictional, foreign, and parent vs. subsidiary, as well as other forms such as partnerships, proprietorships, joint ventures and nonprofits.

Understanding the size and complexity of the enterprise, the multijurisdictional aspects of its business, and the specific audit and assurance requirements will increase the effectiveness of IT audit and assurance professionals, the work they perform and the usefulness of the resulting reports.

GOVERNANCE

The IT audit and assurance professional should understand the governance structure and governance processes—including the enterprise’s organization and where each business unit and supporting function fits within the enterprise’s structure—as well as the lines of authority and reporting. In addition, the audit and assurance professional should have a firm grasp of the roles and responsibilities of each level of management, where these are defined, for example, in position descriptions and job/committee charters; how they are operationalized; and how compliance is monitored.
This would involve gaining an understanding of the enterprise’s governance processes from an enterprise perspective, including board of directors, executive and line management, and technology. Further, it would involve gaining an understanding of the roles and responsibilities at various levels throughout the enterprise and how the various roles contribute to an effective governance process. Additionally, an understanding of governance will require gaining an understanding of the enterprise’s policies, procedures, standards, practices, guidelines, directives and other information that establishes the operating infrastructure of the enterprise, as well as an understanding of the accountability and reporting structure. Finally, the IT audit and assurance professional should understand the enterprise’s risk appetite—how it monitors, assesses and addresses risk and how it deals with uncertainty.

LAWS AND REGULATIONS
Legislation, regulations and rules play an important role in structuring the enterprise’s business processes and practices by providing guidance and direction, as well as requiring compliance. By understanding the legislative and regulatory requirements and their impact on the business processes, the IT audit and assurance professional is better able to appreciate the boundaries placed around the enterprise’s operations and the requirements to comply with various rules and regulations.

The IT audit and assurance professional must also consider compliance requirements when scoping audit, assurance and advisory assignments. Failure to understand and consider the legal implications could make the IT audit and assurance professional’s work less relevant or even inaccurate or unusable.

BUSINESS PROCESSES
IT audit and assurance professionals should understand the day-to-day business processes inherent in any business. They should comprehend the physical activities involved in each business process, as well as the information acquired, documented and used in that process. Further, they should understand the flow of that information throughout each process and the controls over the information to ensure its integrity.

Core business processes include acquiring resources, making products, marketing and selling products or services, collecting money, and reinvesting in the enterprise’s core processes. In addition, the IT audit and assurance professional should understand the enterprise’s process for monitoring and controls established to ensure appropriate performance. Core business activities could also include research and development, as well as methodology and software design and development to enable the enterprise to improve existing products and services or develop new ones.

The IT audit and assurance professional should also understand the other business processes in which the enterprise engages. While these are not core business activities, they are required to sustain the enterprise. These include securing capital, financing operations, recruiting and managing staff, computing and paying taxes, and other supporting activities.

As previously indicated, the IT audit and assurance professional will likely encounter situations that require increased knowledge of external environments, such as industry standards or technical requirements, legislative and regulatory obligations, and their impact on the enterprise’s business processes.

OPERATIONS
The IT audit and assurance professional should understand basic business models—such as the Cont’l model of Plan and Organize, Acquire and Implement, Deliver and Support, and Monitor and Evaluate, or the ISO model (based on the Deming cycle) of Plan, Do, Check, Act—that can be applied to an enterprise’s operations.

Further, IT audit and assurance professionals should relate the models to their own enterprises to understand their enterprises’ business life cycles. In doing so, they should identify key process documentation used in monitoring and controlling operations and the key reports relied upon by management to monitor and evaluate these processes.

Key operational processes may include inventory, manufacturing, sales/order entry, purchasing, payroll, receivables and collections in a manufacturing entity. In the hospitality industry, it may include designing tours, consolidating vendors and managing vacation packages, or arranging entertainment and marketing events.
The IT audit and assurance professional should also gain an understanding of any industry-specific requirements that influence the business process through legal, regulatory, industry-mandated or other criteria. The IT audit and assurance professional should understand not only what is happening throughout the business cycle, but also why it is happening and how it is being performed, including how it is being controlled and reported.

USE OF TECHNOLOGY
Enterprises adopt and use technology differently. The degree to which they use technology, the business processes supported or led by technology, and the approaches and means of minimizing technology risks while leveraging technology gains will impact the IT audit and assurance professional’s approach to an assignment and, accordingly, the knowledge and skills required.

Figure 3 illustrates three stages in the business use of technology: support, enabler and business-centric. Technology used to support business processes is the basic level, and may involve typical financial and administrative processes. At the enabler level, the business is using technology to extend business processes to achieve greater efficiency, effectiveness or cost savings. At the business-centric level, the use of technology is an integral and critical component of the entire business, for example, an e-commerce business.

By using the table in Figure 3 as a means of classifying the business use of technology, the IT audit and assurance professional can determine the sophistication of the technology environment and the knowledge and skills required to conduct an effective audit.

FINANCIAL
Financial information, whether developed for regulatory or statutory reporting or for managing specific operational and business processes, is a critical element of any business. Financial information must not only be complete, accurate and timely, but must also be relevant, in that it meets the users’ needs and allows them to appropriately manage the business.

IT audit and assurance professionals should understand the “flow of the numbers,” just as they should understand the physical flow of goods and the corresponding flow of information involved in each business process. This will require a basic knowledge of accounting—the debits and credits, and the accounting for each business process.

The IT audit and assurance professional should also understand the methods and rationale for recording financial transactions within each business process, such as sales, deferred sales, product development costs and amortization of product costs. Further, the IT audit and assurance professional should understand various accounting processes that record costs, such as standard cost, job cost and process cost methods of accounting for manufacturing processes, as well as the treatments of overheads.
The IT audit and assurance professional should also understand how basic business accounting results in three types of reports:

- **Financial reporting**—Allows the enterprise to comply with statutory reporting requirements, such as quarterly and annual filings with stock exchanges
- **Regulatory reporting**—Such as to taxation authorities, utility regulators, or insurance and financial regulators, allows the enterprise to demonstrate compliance with specific requirements
- **Operational reporting**—Provides senior management, supervisors and line managers with information to control business processes, as well as to report various operational information to senior and executive management

**BUSINESS MEASUREMENTS**

Every business needs a method to measure progress and accomplishments. IT audit and assurance professionals should understand the fundamentals of establishing business goals, strategies and plans. They should also understand the various ways to measure progress and attainment of business goals throughout the enterprise, and how to roll these up for executive and board reporting.

Knowledge and skill in measurement techniques, such as return on investment, net present values, discounted net present value, payback period and discounted cash flow, to name a few, are required to ensure that the information being provided to management is appropriate and relevant for the business purpose.

Knowledge and competency in these eight areas will provide IT audit and assurance professionals with a solid foundation of business processes to enable them to deal with technical issues from a business context and to communicate observations, findings and analyses, and develop effective recommendations for boards of directors, executives, and senior and line management.

**GETTING STARTED**

There are a number of considerations to be addressed prior to embarking on a program to provide IT audit and assurance professionals with business knowledge and training. They include:

- The individuals’ current level of business knowledge and skill
- The anticipated use that the individuals will make of the business information and skills obtained
- The type of work to be conducted and the degree to which that work will require and/or benefit from increased business knowledge and skill
- The culture within the enterprise with respect to education and training
- The structure of the department or area in which the IT audit and assurance professionals work and its relationship with the board of directors and executive management, for example, the reporting protocols and meeting attendance requirements

These business skills are in addition to the other skills required by the IT audit and assurance professionals, including communications, relationship management, interview, analytical, and dealing with resistance and difficult situations.

While many enterprises will welcome the additional business knowledge and skills possessed by the IT audit and assurance professionals, others may see it differently. Such skills may well suit IT audit and assurance professionals in providing advisory services, more than those performing technical tasks in support of a compliance audit team.

Entities should consider carefully the purpose and rationale of equipping IT audit and assurance professionals with increased business knowledge and skills. Providing education and training to equip IT audit specialists with business skills that may never be used, or that will detract from their other skill sets, may prove to be detrimental to the individuals’ careers and the enterprise’s management of their expectations. Conversely, keeping IT audit and assurance professionals in technical roles that limit their ability to master new skills and grow within the enterprise will likely be equally detrimental.

Accordingly, each situation must be carefully weighed and a balance must be obtained.

**ISSUES AND CONCERNS TO BE ADDRESSED**

Identifying the issues to be overcome in ensuring that IT audit and assurance professionals are fully equipped with appropriate business knowledge will require that they not only understand the issues, but also how to address effectively any risks or deficiencies through recommendations that are logical, practicable and business-focused.

Issues and concerns to be addressed include:

- **Technology focus**—Potential IT auditors recruited from a technology/computer science background may lack even basic business knowledge and skills. Their strengths may...
lie more in the area of technology than in business and, accordingly, they may thrive on the technology more than the business issues and may not want to dilute their highly focused technical skills.

• **Resources and time**—Enterprises may lack the time, talent, and financial and other resources to add business knowledge and skills to the knowledge base of their technically focused IT auditors.

• **Team concept**—IT audit departments and, in particular, general audit departments may operate on a team basis, with general auditors providing the business knowledge and the IT auditors providing their technical skills to the general audit team, thus limiting the IT audit and assurance professional’s overall involvement in the business aspects of the audit. Additionally, IT audit reports may be drafted by technical IT audit and assurance professionals, but edited and presented by the general auditor, thereby limiting the need for the IT auditor to “speak business.”

• **Specialization**—IT audit and assurance professionals may focus on one particular technology, business unit or business process, and, accordingly, management may be concerned that the IT audit and assurance professionals would not have an opportunity to use the additional business skills.

• **IT audit and assurance professional’s career**—A number of IT audit and assurance professionals may want to be involved only in the “techie” side of IT audit and assurance work and may not naturally gravitate to the business issues.

• **General auditor perception**—The general auditor may have a perception of the IT audit and assurance professionals as only technology specialists. Therefore, the IT audit and assurance specialists may not be invited to key meetings or may be precluded from participating in the business communications process, thereby limiting the perceived need for, and opportunity to engage in, business-focused discussions.

• **Executive and management perception**—Executive and management may be unwilling to entertain the idea of increasing the IT audit and assurance professional’s knowledge or expanding the IT audit and assurance professional’s role.

• **Expectations of IT audit and assurance specialists**—The expectations of management and others may vary; they may consider “IT audit” to consist of three roles:
  - IT audit control specialist (e.g., security, control, privacy)
  - IT audit technical specialist (hardware/software)
  - IT audit systems/application development specialist

A lot of the focus may be on the development specialist as a value-add in supporting an enterprise’s systems development projects, with less focus on the very technical hardware or software IT audit specialists’ role.

Conversely, with the increased importance of security, controls and privacy, management may prize the IT audit role in supporting its controls reporting. A lack of clarity or frequent shifts in the enterprise’s expectations of IT audit and assurance specialists may either encourage or stifle the IT audit and assurance specialist’s ability to obtain business knowledge and skills.

Given that the enterprise can successfully address the issues and concerns and can develop a career path for IT audit and assurance professionals that includes the continued and increasing effective use of their business and technical skills, developing individual career paths, including an increasing business focus, would appear appropriate. This will involve assessing current business skills, identifying appropriate sources of training, ensuring that training is provided and that the IT audit and assurance professional is progressing, and developing the appropriate skills for use within the enterprise.

**ACQUIRING BUSINESS SKILLS**

There is no shortage of places where business knowledge is available. There is no shortage of people willing to teach business skills. However, finding the right combination that allows the IT audit and assurance professional to acquire the appropriate knowledge and the skills to use that knowledge effectively within an audit, assurance or advisory role can be difficult.

While continuing education seminars and courses, executive or part-time business degrees, training weeks, and retreats are ready sources of business information, their cost and time commitment may not be affordable or warranted in all cases.
Other sources such as industry groups, night school courses and certificate programs should be considered. Businesses themselves can create opportunities for IT audit and assurance professionals to acquire business skills—through job shadowing, job rotation and mentoring programs.

CONCLUDING THOUGHTS
IT audit and assurance professionals bring considerable technical skills to audit, assurance and advisory assignments. Their participation provides additional insight, a technical perspective and identification of technical issues, concerns, problems and solutions to any assignment. Their participation increases the effectiveness of the assignment by including technology-related risks and threats, increased insight into potential causes and impacts, and heightened awareness of the pervasiveness of technology in most business processes.

With technology embedded in most business processes and with reliance on technology being critical, the lines between business processes and technology processes are becoming blurred.

Does it still make sense to treat IT audit and assurance work as a separate component of audit and assurance assignments? Would it not be better to equip IT audit and assurance specialists with business skills to allow them to more fully understand all of the business issues and impacts and provide them with the skills to communicate effectively with boards of directors and executive management?

Providing IT audit and assurance professionals with increased skills to enable them to assess the business, as well as the technical aspects of an issue, would benefit both the professional in terms of career satisfaction and also the enterprise in terms of the quality and relevance of the analyses performed and the recommendations made.
Building Your Bridge to the Future

First, the bad news. The IT sector, which has been immune to many previous downturns, has undoubtedly been hit this time. While booming sectors like banking led the dive down to bust, economic turmoil spread across all areas of the global economy. Entire companies—and their IT staff—have been eliminated in this recession, while IT professionals have not been immune from across-the-board cuts in other organisations that survived the initial shock.

For many IT professionals, this is the first time in their career they have had to face a potential lack of demand for their expertise. Nearly four decades of unbroken growth seemed to judder to a halt at the end of 2008. Since then, some have experienced six, 12 or even 18 months of unemployment without being able to secure another role.

Of course, most people have retained their permanent or contract positions. Yet, many have found that salaries and rates have been frozen or even cut by 5 or 10 percent—occasionally by as much as 30 percent. Many who have kept their jobs are finding that they have to achieve more with fewer resources, but they feel too insecure to look for jobs elsewhere. Things are tough.

GOOD PROSPECTS FOR IT PROFESSIONALS

However, the shock of the initial crisis has passed, and good news is returning. What’s more, it is IT professionals who are benefiting most from current developments.

For a start, the IT function is now acknowledged as the central driver of the entire organisation. Reed research amongst more than 600 employers in 2009 found that IT was less hit by cuts than any other function within organisations apart from the human resources (HR) profession. Fewer than two in five (18 percent) organisations made IT cuts, compared to 26 percent that cut core operations staff and one in three that cut administrators.¹

At the same time, a fundamental shift has occurred in demand for IT expertise.

During the boom, investing big money in cutting-edge technological development was seen as essential to retaining competitive advantage and maximising profits. That was then.

Now, organisations are in a different place. Their priority is to consolidate and protect what they have while maximising performance. Information governance, control, security, risk management and audit are all essential in this environment. These are also the skills organisations need to effectively undertake technology transitions and manage the restructures, consolidations, mergers and takeovers that characterise the current business environment. As stability has returned to world markets, ISACA members are finding that their particular skill set is leading demand for IT professionals.

And the good news is growing. Having led the dive down, the banking and finance sector is currently leading recovery in many countries. Other areas are also returning to health, and new sectors and entire economies are growing. IT professionals who spend time preparing themselves now will be ready to benefit from new opportunities as they arrive.

NEED FOR PROFESSIONAL CERTIFICATION AND DEMONSTRABLE EXPERIENCE

In this still uncertain context, employers need reassurance—and quality assurance above all—when they recruit new expertise. Professional certification provides this. Membership in professional associations and possession of a range of specialist qualifications are now minimum requirements for many key roles. If, as an IT professional, you are aware of gaps in your qualification portfolio or additional certificates that would add to your range, now is an excellent time to acquire them.

James Reed, FCIPD,
is chairman of the Reed Global group of companies, the recruitment specialist firm founded by his father, Alec Reed, in 1960. The group comprises Reed Specialist Recruitment, Reed Online recruitment, Reed in Partnership and Reed Learning, and spans Europe, the Middle East and Asia-Pacific. In January 2010, Reed was named as preferred bidder to deliver the UK Government’s Backing Young Britain campaign. He is also a member of the UK Government’s National Employment Partnership, which was set up in January 2009 to identify what more can be done to collectively help people and businesses cope with the downturn in the economy, and ensure that they are well placed for the upturn. He initiated the Keep Britain Working campaign, which aims to promote innovative ways to preserve and create jobs. The campaign is backed by a broad range of businesses, the prime minister, the mayor of London, all three of the main political parties, the British Chambers of Commerce and the Trades Union Congress.
However, simply holding the requisite professional certification and listing the technologies, processes, ISO standards and frameworks you have mastered are not enough in this competitive marketplace to secure the desired role. As an IT professional, your curriculum vitae (CV) must demonstrate that you have the track record of achievement to go with the qualifications. You must show how your knowledge has been proactively applied to make a difference.

You need to demonstrate your ability to understand requirements and resolve project issues, to identify as well as report on critical areas, and to design and implement solutions that encompass processes and procedures as well as technical fixes. Surprising words such as ‘flexibility’ and ‘creativity’ are now featured on successful CVs, alongside examples of a results-driven outlook. If you can add evidence of times you have succeeded in thinking ‘outside the box’ to deliver more with less, so much the better.

**NEW FOCUS ON MEETING STRATEGIC GOALS**

Information governance, control, security and audit functions may have proved their importance in the current climate, but more than ever before, they need to demonstrate how they contribute to achieving the organisation’s strategic goals.

Frameworks developed by ISACA, such as Risk IT and, of course, Val IT™, demonstrate exactly this approach. At this stage, recruiters may be less familiar with these specific qualifications than they are with the more established International Organization for Standardisation (ISO) standards and ISACA’s CoIT framework, or certifications such as the Certified Information Systems Auditor (CISA), Certified Information Security Manager (CISM), Certified in the Governance of Enterprise IT (CGEIT) and Certified Information Systems Security Professional (CISSP).

However, those who demonstrate their awareness of this approach and its effectiveness will stand out during the job assessment process.

The strategic drive to deliver value goes hand in hand with another key shift in the economic environment.

**INCREASED DEMAND FOR PEOPLE SKILLS**

Fascinatingly, in the current climate, the apparently ‘soft’ people skills are more in demand than before. In complex global environments recovering from turmoil and under more pressure than ever, a proven ability to lead and manage people is critical.

Leadership groups need to be created and developed. Policies on change programmes, performance management and communications need to be agreed upon and implemented amongst specialists under pressure. Expert teams need to be motivated, coached and developed more, not less, in the current climate if they are to keep delivering to their full potential.

Problem solving in this complex environment requires a proven ability to manage relationships with internal and external expert stakeholders. ISACA members, supported by their chapter networks, have particular skills in managing relationships amongst their own peers, from technology risk managers, control and security experts, and group financial governance specialists, to internal and external audit specialists. This environment also makes it even more essential that IT governance, strategy and practice are wholly aligned with board strategy and decision making. Whatever your speciality, you need to build on your authority and embed your ability to manage upward, to maximise your effectiveness for the business as a whole.

**EXPLORE NEW DIRECTIONS**

In spite of growing demand, difficulties remain. Some IT professionals who have retained their jobs feel their careers have stalled. A key minority of those who are unemployed feel traumatised by job loss and marooned in unemployment.

In this situation, IT professionals need to take an active, strategic look at their career options. This is their opportunity to plan a new career path to meet both their immediate needs and their longer-term career aspirations.

As an IT professional, you should take comfort in the fact that the underlying demand for your professional skills is high and on an upward trajectory. However, this is not a time to be complacent. Things really have changed. This means you have to be open to change as well and be prepared to develop your mind-set as well as your skill set to secure the best new opportunities.

First of all, you must get the basics right. You must:

- Make sure that your existing CV is fully reworked to meet the new priorities of today’s employers.
- Demonstrate how you have put your expertise to work, with specific, evidenced examples of achievement.
• Ensure that you include positive words to describe your ‘soft’ skills, strategic leadership and management achievements on the CV.
• Use available time to add new skills.
• Take steps to address gaps in your lists of professional qualifications, memberships and certificates.
• Benchmark your CVs against those of peers, and keep on revising, tightening and improving them.

At the same time, you must actively open your mind to new possibilities. You must start from your own experience. What have you enjoyed? What drives you? Where do your passions lie? Where would you ideally want to be in five years time? You must set out your best vision for everything you want your career to bring to you. You must not be afraid to think big.

You should utilise this springboard:
• Use the energy and motivation it provides to research the current market for your skills.
• Take every chance you can to get involved with others to understand more about what is happening in the wider economy.
• Maximise the tools at your disposal, for example, ISACA’s excellent career advice portal and vacancy board (www.isaca.org/careercentre).
• Cultivate relationships with recruitment specialists, and quiz them about what is really going on—especially new trends and opportunities they may spot before everyone else.
• Exploit the global power of the Internet to the fullest.
• Research demand for your expertise through both niche and international jobsites.
• Above all, network with fellow professionals from your local ISACA chapter, for example, for their understanding, support and, more than anything, their knowledge of potential new openings.

From this, if you are looking for employment, you will be able to map out the best opportunities.

CHANGE ONE’S MINDSET FIRST
Remember, if a fundamental change in the wider economy has stalled your career as an IT professional, you may need to dramatically change your attitude—mind-set—to open yourself to new opportunities.

If, for example, as an IT professional, you have always had permanent roles, now is the time for you to consider contract work, especially since this sector is most in demand as organisations emerge from recession. If you are an established contractor, you can build on your flexibility and wide range of experiences to explore different options as they emerge.

Here are three additional, and fundamental, shifts in direction to consider.
• Change sector—If the core industry sector in which you have built your career to date has stalled or shrunk, you must look beyond this. IT professionals’ skills are transferable. If your background to date has been in finance, you can explore demand within retail, manufacturing or pharmaceutical conglomerates. You must do the research. You must check out not only where your qualifications are in demand, but also the sector-specific language employers are using to describe what you need, and then you should use these descriptive terms on your CV to demonstrate interest and understanding of each new target sector. You should work out where your transferable experience and skills lie, and then frame these in new ways to demonstrate your value in different contexts.
• Change location—The marketplace is now global, yet growth in home markets means that many have never before had to explore the personal implications this might have for their own careers. For example, candidates from the US are seeking out and embracing exciting opportunities elsewhere in the world. While growth has stalled or slowed in parts of the US and Europe, other economies such as Australia and New Zealand have recovered much faster. Tax-free openings in the Middle East or in the fast-growing Tiger economies of Asia-Pacific, led by Hong Kong, are increasingly attractive options. Demand for the technical, managerial and strategic skills of IT professionals who are interested in relocating to a whole different continent is high.
• Expand aspirations—Support these with extra skills. After completing a self-assessment, you may find that it leads you to explore a completely new direction for your life and career. You may consider adding a whole new expertise to your existing skills. Adding accountancy qualifications, for example, to IT skills opens up a whole range of career options in high-demand areas, such as forensic analysis. To do so, you may need to add evidence of ‘soft’ skills by taking courses in negotiation, relationship management or leadership. Gaining a Master of Business Administration (MBA) would demonstrate your strategic
business acumen. You can build on your networks to set up your own consultancy or even launch a business start-up. As an IT professional, your proven ability to lead others and meet business goals may mean now is the right time to make that move from chief information officer (CIO) to chief executive office (CEO).

CONCLUSION

The first priority, when seeking a career move, is to keep taking the practical steps that will continue to move one forward. Even the smallest step will help build confidence and help lead to the next. Research shows that employers will recruit people with the right attitude—the right mindset—over and above those with better skills. Demonstrating grit and resilience will put you in the best state of mind to demonstrate these vital qualities to potential future employers.

You must remember that this is a journey to the next stage in your career. Yes, you should expand your networks, explore existing and new markets, identify where demand is highest for your skill set, target areas of growth, and continue to hone your CV. At the same time, the next job could take you in a direction you could never have anticipated. To maximise success, you should try to enjoy the journey as much as possible, and, above all, keep your mind open to explore all the new opportunities that will come your way.

ENDNOTE

1 Reed Global, ‘Meeting the People Challenge: How Are Employers Responding to Recession Today, Compared to Two Decades Ago?’, produced by Reed in support of Keep Britain Working, September 2009

EDITOR’S NOTE

ISACA is developing the Career Guide for Information Security and Assurance Professionals, which will be available to the public as a complimentary PDF download on the ISACA web site. Please look for its availability by midyear. Once available, please look for it at www.isaca.org/deliverables. To learn more about ISACA research projects in development, please visit www.isaca.org/research.

SharePoint Deployment and Governance Using COBIT® 4.1: A Practical Approach

This book contains a comprehensive, step-by-step guide on how to practically deploy and govern SharePoint 2007 and 2010 using COBIT® 4.1. This practical guide blends the needs of the deployment staff and audit teams with a comprehensive blueprint that puts business in charge. The book is filled with authoritative tips, techniques and advice.

For additional information and complete descriptions, see pages S1-S8 in the Journal or www.isaca.org/bookstore.
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 June/December 2010 exams, 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 understanding 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 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 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.
Information Security Career Planning: Education, Training and the Role of Professional Certifications

A conversation on information security career planning must be framed around the evolution of the industry. Security evolved from a glass house model in which there were few systems, few applications, few users, and few key requirements beyond accounting for resource usage. Security could be handled as a simple administrative technology task that made sure users and resources did not conflict with one another. The knowledge and expertise required to perform IT functions, including security, mapped to only the most basic technical skills.

For many years, security stayed largely static as technology advanced at an accelerated pace. For many businesses, reliance on mainframe hosts gave way to client-server-based networks and applications, and then to external connectivity. Later, Internet connectivity became the norm, and the data that had once been easily protected in one place were spread across the organization, and exposed well beyond. The increased use of technology to manage information produces the greatest risks. Industries have gone through several cycles of disruptive innovation in which security was impacted.

The security function remained chained to its IT heritage in the days of glass-house data centers, and practitioners had neither the skill nor the authority to effectively protect the emerging corporate landscape. Security was primarily buried within the technology organizations of most companies with limited visibility to or understanding of business practices. Security was seen as a necessary evil and an expense, so access to budget and resources was usually limited. During the evolution of the security function, in the 1980s and 1990s, security was a part-time role filled by IT practitioners who understood network technology.

Only in recent years has the security function garnered more visibility and been seen as anything more than an enforcer peddling fear, uncertainty and doubt. Significant regulatory changes around data protection and privacy standards have raised security concerns to the board levels of most public companies, but the availability of properly skilled resources is sorely lacking. It is important that security practitioners have a strong understanding of regulations and that they be prepared to link security efforts to compliance. There has been a long-standing gap of “softer” skills in the information security profession.

Even today, most information security professionals have come from a purely IT background. It has been only in the last decade that certification, training or an academic concentration in security has become more common. However, initial offerings have been highly technical—focusing on system and network controls such as encryption and firewalls. They have been “teaching information security” and have not broadly evolved to “teaching information security management.” Often, the education has not kept up with the regulatory demands of the corporate world. Newly minted security practitioners can implement tools to improve controls, but they cannot procure budget or influence stakeholders to make such tools available.

CAREER PLANNING OPTIONS

Effective career planning depends upon the right types of educational foundations. Businesses require more and more agility in order to make competitive decisions. More frequently, those decisions involve the management of confidential or sensitive data that may be impacted by

Kenneth Newman, CISM, PMP, ITIL/ITSM, is Central Pacific Bank’s vice president and information security manager. He oversees the bank’s information security program and the protection of its information assets. Previously, he served as an online risk manager for Washington Mutual and has managed various global and regional security and risk functions for Deutsche Bank and Citigroup. He has 18 years of progressive experience in technology, security, risk and privacy and a 16-year proven track record delivering risk-based solutions in financial services. Also a frequent trainer, he has presented at local, national, and international events for groups including ISACA, American Banker, Ziff Davis, and ComputerWorld.
regulatory requirements. Poor decisions could produce regulatory fines and sanctions or a breach of information that could erode customer and shareholder confidence. To be successful, the security officers charged with data protection and regulatory compliance need the skills and expertise to respond quickly to these needs and guide the organization to a path that produces an acceptable level of risk. Creating that kind of capability in the next generation of security professionals requires a broad-based training approach.

There are different types of security training available today. Each fulfills certain needs, and companies may use them alone or in combination for different reasons. The most basic type is general industry training. These courses (often tied to conferences) may be anywhere from a few hours to several days in length. They are often technology-independent or may discuss one or more technologies at a very high level. They provide a general introduction to security and are generally geared toward what kinds of solutions should typically be implemented to meet basic security needs. Companies will often send brand new security people or IT people given operational security responsibilities to these types of classes. They may offer a basic introduction to risk or regulatory requirements, but they do not provide the skills to effectively implement or update a security program.

Similar in terms of time and cost, product-specific training is also available. These courses generally focus on a technology or platform, and go into a greater level of detail on a narrower scope. They can teach someone how to do something such as configure a firewall or use security settings on a server operating system. Companies may use this training for IT staff to improve security as a reaction to some issue such as failing an audit or having a system break-in. They may not have a dedicated security team or a comprehensive security program. However, they have an immediate need to improve security, so they identify a basic element to provide corrective action. They implement the solution and provide training to staff to operate it. As with general training, product training does not provide the breadth of skill required for a successful security professional.

Certifications can be general industry, such as Certified Information Systems Auditor (CISA), or product-specific, such as Microsoft Certified Systems Engineer (MCSE). They require a greater educational or time commitment than the types of training discussed already, because they may involve coursework, practical experience and examinations. They provide correspondingly broader and deeper skill sets that may include the application of basic knowledge toward problem solving. Individuals often pursue certifications to enhance job prospects because many employers use them as benchmarks for hiring. Those companies that have a commitment to development may also support IT or security staff in achieving certifications because they enhance an employee’s value to the organization. At their highest levels, these certifications can help someone with broad practical experience support an existing security program, but they still may not provide the ability to step into a role and create or update a program. Further, many without the background or experience can still study (or train boot-camp style) and pass these tests, so certifications alone, while an indicator, are not an absolute benchmark of capability.

Finally, academic education requires by far the most time and financial commitment, but offers the greatest breadth and depth of skills. Individuals may pursue academic degrees when they are confident in their long-term career goals or when they seek to enhance the level of the profession through research and development. Some employers may support this level of personal development, when they understand the clear value that a steady infusion of new ideas, rigorously tested in an academic environment, can bring to an organization. Successful graduates with some practical experience are more likely to be able to implement and influence security programs and, in turn, provide value to their organizations.

To keep matters simple, this article will discuss successful career planning for an information security professional using as its example private-sector corporations with some kind of regulatory requirement for information protection and privacy. Such businesses are revenue-driven and share several common characteristics. They are required to understand and manage risks in their decision-making processes. They also need to be fully versed in the regulations they are bound by to correctly comply with both the letter and the spirit of the law. Such organizations are also marked by a need to effectively communicate internally and externally with various stakeholders to manage their public reputations. Finally, they usually also enforce a strict culture of cost containment to maximize their profit generation. This basic organizational profile will be used to establish what kinds of elements are most beneficial for successful career planning.
KEY ELEMENTS FOR SUCCESSFUL CAREER PLANNING
Regardless of options, there are some key elements that should be present in any form of education in order to provide lasting value to the information security professional. This article does not discuss technical details, although they are acknowledged as core to almost all levels of security professionals. Instead, the article focuses on those areas that create a “breadth” of softer skills in order to produce a more well-rounded and marketable individual.

Understanding Risks
Risk must be every information security practitioner’s benchmark. It is one of the five components required for internal controls under the Committee of Sponsoring Organizations of the Treadway Commission (COSO) Internal Control—Integrated Framework. Risk analysis is a key requirement—not just an ability but as a primary task such as creating policies.

The days when security managers could see the world in black or white, yes or no, are long past. Security for the sake of security is never viable in the corporate world. There must be a risk-based reason behind every decision. This can be especially challenging in larger organizations in which different business areas have different risk appetites.

The starting point should be in the company’s policy and procedure framework. This is where the security professional documents a baseline—if one is not already specified there. Then, they must make sure business owners understand those risks and have measures in place to manage them effectively. Past strategies designed to sell fear or blind compliance are outdated. This is also not an isolated exercise. True risk management is a macroprocess in which the security professional maps risk across the organization.

The value here is straightforward. Expenditures for excessive security can and should be avoided and business operational impact can be minimized.

Interpreting Regulations
Regulatory compliance is the absolute benchmark against which the success of a security program will be measured. The subjects of law and regulation are fast becoming a specialty unto themselves within the field. All publicly traded companies in the US are governed by one or more regulations. In some cases, there may be multiple regulations in multiple jurisdictions. More and more, these regulations include provisions for security that must be balanced against the risk appetites discussed previously. However, regulations seldom spell out exactly how to do something. They just imply what kind of goal is to be achieved.

General regulations have to be mapped to increasingly more detailed governance frameworks, control objectives, and, finally, individual controls. There is power here. Management may not always care about technical security, but they always care about regulatory compliance. The requirements provide an opportunity to get management’s attention and focus it where the risks are. Understanding is also important because different areas of an enterprise (e.g., legal, compliance, risk management) may have different views that the security practitioner needs to be able to integrate.

Communicating Needs
Communication is another one of the five components required for internal controls under the COSO framework. An information security role in an organization may exist only on paper as a box in an organizational chart. The position may actually have no practical power or authority. As such, one of the most important tools to be taught is how to communicate in a meaningful way with nontechnical personnel, i.e., managers.

The practitioner will understand risk and the importance of security, but the manager may or may not even care. The real job of information security is to overcome negative impressions and make sure the manager understands the risk, accepts it, sees its potential impact to the bottom line, and documents appropriate steps to accept or mitigate it. Otherwise, security efforts run the risk of being marginalized.

Security managers rely heavily on training to help business areas handle risk, and making training effective requires strong communications skills. While opinions may differ, the security officer’s goal is to find common ground. In some cases, that may mean knowing when to work with other areas that may have more influence like an audit function. Security professionals must focus on negotiation and collaboration to work within the framework of the organization to ensure that risks are properly addressed.

Managing Costs
Often security groups have very little budgetary authority or financial control. Security products are not brought into an organization because they are new or interesting. Security initiatives must be “sold” just like any other business proposal.
There has to be a specific benefit, reason or return for the investment. In most cases, the security officer has a long list of initiatives and insufficient budget, resources and time. Real-world projects have very different consequences. A project can be successful, but still fail visibly if cheaper alternatives are identified.

They must learn to “know their limitations” within the confines of the organization and prioritize accordingly. Risks will guide where the money goes, and security professionals should be prepared to support other initiatives over their own if they can demonstrate an improvement in security.

Likewise, control or audit requirements should be reviewed carefully. A control is of little value if it is more expensive than the asset it protects, or if it produces too much operational overhead in mitigating the risk. Over time, the goal is to begin to establish a track record by showing improvements with minimal incremental spending. Measurement and metrics are key tools here that can help justify when an expenditure makes sense.

**Understanding Business Operations**
An information security manager must make sure that the organization views security as a business function and the manager as a business partner. An organization’s security program is made up of four basic components: people, processes, products and policies. They all interact together to ensure the program is meeting its goal of providing adequate controls to reduce risk for the company.

For each of those areas to be effective, the information security professional needs to understand how the posture of any them has an overall impact on the organization. To do that, it is necessary to understand how the business operates. This is a fundamental requirement of risk-managed security. Health care companies and retail stores require different levels of controls to appropriately secure their operations. “Common practices” such as frequent password resets abound, but they may not make operational sense in every business area. However, they often appear in audit checklists, and information security professionals have to be ready to explain variations in light of risk.

A security program must take into account the values and priorities of the business to be effective, and a security manager needs the same organizational knowledge as a business manager to add value. From a career standpoint, this, in turn, adds value to the security manager.

**SUMMARY**
Risk management, regulatory knowledge, communication skills, cost awareness and business sense are all different aspects of the need for and ability to provide security controls. Thus, the true benefit to the organization is risk-weighted, cost-effective, compliant, operationally viable controls.

The lack of skill or knowledge in any one area impacts the others and, ultimately, the level of control that a security professional can achieve in their organization. Given the importance of a properly skilled and well-educated security workforce and the variety of educational options, the practitioner should assess education, training and certification choices carefully to choose the best course of action to meet their career goals.

**EDITOR’S NOTE**
ISACA is developing the *Career Guide for Information Security and Assurance Professionals*, which will be available to the public as a complimentary PDF download on the ISACA web site. Please look for its availability by midyear. Once available, please look for it at www.isaca.org/deliverables. To learn more about ISACA research projects in development, please visit www.isaca.org/research.
Audit Careers 2010: The Swing of the Pendulum

The economic downturn of 2007-2010 has had a tremendous impact on auditors’ careers in comparison to other recessions.¹ Using the analogy of a swinging pendulum, the auditor’s career has gone from one extreme to another—from internal audit’s rapid expansion during the implementation of the US Sarbanes-Oxley Act-required controls, to the alarming contraction of the number of employed auditors during the recent recession. Now, the pendulum is beginning to swing slowly back toward an expansion phase.

In previous recessions in the US, internal audit functions were not always affected. In fact, in the downturn in the US of the early 1980s, many audit departments actually grew in headcount, possibly as a result of corporate leaders realizing that fraud is more prevalent in down times and feeling concerned about the lack of reliable controls on computerized accounting systems. On the other hand, the recession that followed the aftermath of 2001 shook audit departments as well as every other department. Shortly thereafter, there was a great deal of outsourcing of internal audit to public accounting firms.

The passage of the Sarbanes-Oxley Act in 2002 was a harbinger of happier days returning to the audit world, and within a year, firms were scrambling to try to come to grips with the strenuous requirements of the new law. After just about every available auditor had been pulled into performing Sarbanes-Oxley work, the IT community started getting recruited to fill the multitude of positions. This was at a time when IT people were in great supply and jobs for IT people were scarce. Offshoring of IT positions had displaced a great many people who had been project leaders, analysts and programmers. These people proved readily adaptable to testing the controls over IT systems.

For a number of years, corporate America could not find enough people with Sarbanes-Oxley expertise. Public accounting and consulting firms expanded their Sarbanes-Oxley compliance departments and hired and trained vast numbers of people. As the Sarbanes-Oxley requirements spread beyond the US, talented people with controls testing knowledge became scarce in many other areas of the world. The demand for auditors, or people who could perform even some of the duties of audit, was at an all-time high.

As the turbulent times of the Wall Street financial crisis approached in the latter part of 2007, the tide was already starting to turn. Many corporations had formed their own Sarbanes-Oxley or regulatory compliance departments, taking some of the pressure off internal audit departments that had been forced to divert many of their resources away from performing audits.

With the collapse of prestigious Wall Street firms such as Lehman Brothers and Bear Stearns, suddenly corporate America started to get the jitters. Hiring slowed to a trickle and companies started looking carefully at spending. Liquidity suddenly took on new meaning. Before long, the international accounting and consulting firms started losing business. Layoffs soon followed. In 2008, the Big 4 public accounting offices began laying people off on an unprecedented scale. Cost-conscious corporations started considering bids from second-tier public accounting firms, some of which were staffed by people who had just been laid off by the Big 4. As the recession deepened, the second-tier and regional firms were forced to institute layoffs as well.

The cutbacks were deep and painful. Audit and advisory service lines in public accounting had, until now, typically been viewed as a “safe” profession. After all, the thinking went, big business is always going to need auditors. Suddenly people who had been planning to someday become partners in public accounting found themselves with a pink slip. At every level, from staff consultant through partner, the unemployment rate among auditors was, for the first time, soaring.
Corporate human resource people were elated to be able to interview a wide range of talented individuals before making a choice for an open requisition. Within one year, the supply and demand ratio had reversed itself. In 2007, a Big 4 IT auditor with a Certified Information Systems Auditor (CISA) designation could have had his/her pick of employers in most large cities. By March 2008, employers had their pick of any number of highly qualified IT auditors. Auditors in public accounting were not at all accustomed to being thought of as a commodity in oversupply.

THE CHANGED JOB MARKET
To better understand the dynamics of the changed job market, a simplistic overview of the two different views of the internal audit career can be considered. Many departments regard internal audit as a lifelong career choice. Other departments, ever growing in number, regard internal auditing as a terrific set of skills with which a career-minded person can launch him/herself into any number of other directions such as finance, accounting, operations or strategic planning. Some departments strike a balance of career auditors and auditors building toward another career.

Whereas government agencies and nonprofits tend to prefer career auditors, the majority of Fortune 500 departments view their internal audit departments as a grooming ground for future leadership roles. The majority of students graduating from the top universities strive to some day hold those top leadership roles. Most of these students regard audit as a stopgap—a great place to learn a corporate culture, develop skills and make important connections from which they can then launch themselves in the directions they want to pursue long term.

With the economic downturn and the numbers of Big 4 people being laid off, the ripple effect was almost instant in universities. Students who had older siblings, friends and accounting alumni unemployed started questioning whether getting an accounting degree or an audit specialization was such a good idea. Students started changing majors to economics, marketing and finance if they continued in business school at all. Many refocused on liberal arts. “Before, internal audit was a guarantee for anyone to get a job so people went into internal audit; now it isn’t, so they’re going into whatever they want to,” says Mark Salamasick, director of the Center for Internal Auditing Excellence, University of Texas at Dallas (USA). “I see a lot of students going into finance just because it sounds interesting to them, although the job market is much worse than for internal audit. So you now find students…going into majors that interest them vs. one that has better job opportunities.”

One cannot discuss the economic downturn without mentioning its effect on non-US students and workers in US audit departments. For a number of years, the H-1B work authorization program in the US had been especially helpful for companies trying to hire scarce talent. It is no surprise that the four biggest employers of H-1B visa-holding professionals were in fact the Big 4 firms. When unemployment among auditors started to occur, the Big 4 and corporate America started stepping away from renewing the H-1B work permits. A great many people who had come to the US to get their business and/or technology educations had found their internships and first jobs with the Big 4. Five years earlier, they would have eventually applied for a green card and, after an arduous process, been granted permanent work status in the US. With repeated rounds of layoffs by public accounting firms, many H-1B visa holders found themselves unemployed and with only a short window of opportunity to find another employer or be forced to leave the country. Not surprisingly, the number of employers willing to sponsor foreign workers practically dried up. Many of these very talented individuals have returned to their homelands, or are working in other countries.

The effect of this implosion in the US is yet to be felt, but there has been a profound drop in the number of non-US students attending US universities. Having all these many talented individuals forced to leave the country will likely some day be described as a terrible brain drain with lasting international effects. The attractiveness of acquiring a US education and an opportunity to work for prestigious organizations has greatly diminished. It might make attracting great talent back to the US at some later point much more difficult. As businesses continue to globalize, the insight and cross-cultural business knowledge that these workers bring will be in great demand. As one US-based university instructor recently observed, “My graduate classes now lack much of the richness we had when international students brought divergent points of view to classroom discussions. Their contribution is sorely missed.”
THE FUTURE

Looking at the immediate future, a few things are very certain. The number of pure IT positions is staggeringly low. More and more technology functions have been offshored to less-expensive areas, and more of these offshore sites are popping up. Instead of everything seeming to go to China, India and Pakistan, Mexico is starting to gain ground. As the IT functions become more globally based, so too does the IT audit work. More and more departments are hiring local IT auditors or consulting firms in the countries in which the work is being done.

Another population of workers that has been displaced is the IT people who came to the audit profession as Sarbanes-Oxley testers. Now that the demands for Sarbanes-Oxley testing have been systematized, many of these people are on the job market. When they apply for mainstream audit positions, they fall short of the requirements. Often they do not have an accounting background or experience performing financial, operational or IT audits, and writing professional audit reports. Their expertise is in testing. Many audit directors say that when they post an audit position, they get inundated with applicants who have done only Sarbanes-Oxley work and cannot step right in and perform the kinds of work needed.

Over the last 15 months, several surveys of global audit departments have been conducted to get an idea of how the profession is evolving and the new directions chief audit executives (CAEs) are charting for their departments. There is no denying that both internal audit and public accounting auditors were hard hit in 2008 and even more so during 2009. Of the respondents to the online surveys, representatives from more than 25 percent of companies reported layoffs.

By way of contrast, more than half of the respondents to one survey in January 2010 expect to do hiring in their audit departments in 2010. “I am cautiously optimistic,” Jarrett Fenlon offers. Fenlon recruits for some of the biggest firms in the northeast US. “IT audit positions are starting to show up in ever-increasing numbers. The big firms—Fidelity, JP Morgan Chase, Fannie Mae, Morgan Stanley and State Street—are all starting to feel more confident in their hiring. But, this will not be business-as-usual hiring. The rules of the game have changed—perhaps forever. Although the recession is widely regarded as being over, the recovery is going to be a slow process. Audit budgets are going to be carefully scrutinized and requisitions to hire will be thoroughly examined. Most audit executives have resigned themselves to the fact that they are going to be in a position of having to accomplish more work with fewer resources. The responsibilities of internal audit departments are shifting. They are not as enmeshed in Sarbanes-Oxley work, and the schedule is now moving to other priorities with much more emphasis on value-added services, and that value is best if it shows up on the bottom line of the company rather quickly.”

TECHNICAL DEPTH

Shedding Sarbanes-Oxley responsibilities is freeing up more time for auditors to get back to some of the areas in which they were previously excelling: conducting application audits of the new business areas into which the business has expanded, enhanced fraud reviews, and shrewder utilization of data analytics to help management make informed decisions. Employers now want to hire people who have more ability to accomplish a broader range of responsibilities. The CAE of one Fortune 50 company put it this way, “The ideal person to join our department is a Big 4 CPA who also has experience in industry and has some degree of specialization in the needs of our company—either in terms of product knowledge, market niche or technology deployment.”

As one senior director in a consulting firm said, “The prevailing wisdom is that Sarbanes-Oxley makes you stupid. People who have focused too narrowly on Sarbanes-Oxley work are having a very difficult time proving their adaptability, and often are not really able to articulate how their work directly improved the bottom line of a company—which is critical in today’s environment.”

“IT auditors were once regarded as the scarcest skilled professionals in audit departments,” shares Trish Mulholland, who advises audit groups on the US’s west coast on hiring. “Now some departments are looking for an IT auditor who has even more skills. As departments are evolving into integrated teams, even the IT person is more marketable with a Certified Public Accountant (CPA) certification. If an individual has a technology degree and three to five years in IT audit, companies are attracted to their skill sets, but in terms of long-term career planning, these same employers voice concern about where these people can move in the organization, especially when they have no IT people working in the [US].” The integrated auditor, on the other hand, has the option of moving out into the controllers’ group or into the finance department.
“What I see happening,” opines Caitlin McGaw, a UC Berkeley MBA with experience in several global organizations before joining Lander International a dozen years ago, “is less demand for generic IT audit skills and more demand for specialized abilities such as reviewing enterprise resource planning (ERP) portals, firewalls and penetration testing. At the same time, there is an emphasis on business knowledge and outstanding communication skills. Today’s IT auditor needs technical depth, but also has to be able to expertly build the business case for controls which can be clearly communicated to management inside and outside of audit.”

This is a tall order. But internal audit departments with constrained budgets (a fact of life for the foreseeable future) are looking for a big bang for their buck. IT auditors looking for a new opportunity need to be attentive to these requirements when interviewing, especially when the competition is so stiff.

“Not possessing a certification in this marketplace is a killer,” Michelle Maltzahn adds. “Audit departments want the best and brightest, but they also want the most dedicated people. When a candidate says he was too busy to sit for a certification exam, it just does not ring true. If a person has been laid off, the best advice I give them is to start studying. Take advantage of this time period to pass certification exams, continually read books and stay on top of all the latest technologies that are gaining popularity. Every employer wants to know, ‘How did you make maximum utilization of your time between jobs?’ and you should have a terrific answer.” Maltzahn specializes in recruiting for the Texas (USA) marketplace, but she is quick to point out that the demand for certifications is universal. “And, do not rest on your laurels. Do not settle for just one; continue your education and your dedication to expanding your knowledge.”

The career direction one is seeking should determine which certifications to pursue. The CPA often creates a pathway to directing an audit function. The CISA shows a breadth of knowledge in audit, risk management and technology controls. The Certified Information Security Manager (CISM) demonstrates one’s ability to plan and manage complex, structured endeavors, both in audit and in operations and IT. There are also certifications in specialized areas, such as the Certified Information Systems Security Professional (CISSP) or the Certified Fraud Examiner (CFE), that can help open specific career doors. Not having any certification may result in an otherwise qualified person being locked out of career opportunities.

WHAT HAPPENS NEXT?
The question that many human resources (HR) people and professional auditors are starting to consider is, “What happens next?” Most people who lost their employment during the cutback cycles have landed other positions, but how many of these people consider themselves underemployed and/or underutilized? A great many of the Big 4 displaced people took positions with small and medium-sized companies that soon may be unable to deliver the career plans that these individuals have in mind. Some short-minded employers have harmed their long-term retention goals by offering less-than-standard wages, taking advantage of the supply of talent being temporarily so large. It is no secret that many Big 4 executives are keeping close tabs on where their former employees landed after being laid off. Prudent internal audit departments are taking steps to ensure that they can retain their good talent once the economy improves.

What is the best advice for IT auditors who find themselves out of work?

• Do everything possible to become marketable.
• Create a marketing plan and develop a personal brand and professional network.
• Be prepared to discuss all the value-added services you have provided in the past, and do enough research to be able to offer suggestions of how you can do the same for a future employer.
• Do not carry a chip on your shoulder and expect anyone to make up for the fact of the recession. Layoffs have happened to a lot of people in audit in the last two years.
• Be prepared to explain how you have made the most of an opportunity.
• As much as it might bring temporary comfort to sit at home, go out and be productive. Volunteer, improve your social circle of valuable contacts, visit previous audit departments in which you have worked to find out what changes are afoot in the profession, and attend monthly local
professional meetings for IT auditors or any new field you may wish to investigate.

• Keep moving and keep improving.

In surveying the career prospects for IT audit professionals in the future, the outlook is improving dramatically over what it has been for the last couple of years. This will be a watershed time for people to develop new skills and add value in ways that auditors 20 years ago would never have considered. As the need for security over computerized systems increases, auditors with technical security skills will have ample opportunity to move into security careers. Individuals with strong data analytics skills will be worth their weight in gold.

It is not impractical to think ahead to another age of looming auditor scarcity. With the number of Baby Boomer retirements in the US taking its toll and the diminished number of students that will be graduating with appropriate degrees to enter the audit profession, internal audit departments may soon be faced with the swing of the pendulum toward auditor scarcity. Attracting and retaining talented individuals while staying on budget may be the largest challenge of the next several years.

ENDNOTES

1 This is based on the author’s experience, having guided and directed an executive search firm specializing exclusively in audit positions through three previous recessions.

2 Throughout the last 30 years, Lander International has held weekly meetings among its executive directors to discuss and analyze the trends and changes happening in the audit profession. The directors of Lander International LLC have visited over 300 internal audit departments to put on seminars, teach classes, review audit approaches and gain a better understanding of new directions the profession has taken. It is from these relationships that the quotes used in this article are derived.

EDITOR’S NOTE

ISACA is developing the Career Guide for Information Security and Assurance Professionals, which will be available to the public as a complimentary PDF download on the ISACA web site. Please look for its availability by midyear. Once available, please look for it at www.isaca.org/deliverables. To learn more about ISACA research projects in development, please visit www.isaca.org/research.
It’s Not Easy Being Green: How the Green IT Movement Is Impacting Careers in IT Audit

Political and social mores of the last few years have given rise to a myriad of corporate initiatives around corporate social responsibility (CSR). As the economic recession became more severe, the focus on bottom-line performance took precedence over many of the well-meaning, but costly, CSR initiatives. One large exception to this, however, has been “green IT.” Green IT initiatives occupy a unique intersection; they accomplish socially responsible goals, while providing hard monetary returns on investment and improved financial performance. Thus, while some CSR programs have been shelved in anticipation of future funding, green IT programs have been pursued enthusiastically.

The results are mixed. Some organizations have reported substantial progress and significant gains through IT initiatives, while other organizations have been less fortunate. What makes a green IT program successful depends on a variety of factors, which vary greatly from organization to organization. This article will not attempt to tackle that challenge, as intriguing as it is. Rather, this article will assume that green IT initiatives will continue, at least in the short term, and will focus on how this evolution of green IT will impact the IT auditor’s professional career.

This isn’t the first time IT auditors have had to contend with a rapidly evolving IT environment. The migration to client-server-based enterprise resource planning (ERP) systems, year 2000 conversions, and the advent of e-commerce and the extended enterprise have had major impacts on corporate IT environments. These changes challenged IT auditors who had to reengineer their skills and approach to auditing. Simultaneously, these changes created opportunities for IT auditors to grow their careers in satisfying ways.

The green IT movement is no different. Those IT auditors who seize this opportunity and evolve will likely be more successful than those who do not.

How will the green IT movement impact careers in IT audit? As with some of the aforementioned evolutions (e.g., ERP implementations), the changes will take numerous forms, each with various levels of complexity. Some green IT initiatives (such as virtualization) could individually represent multiday training courses for the IT auditor. This article identifies a few of the major changes to provide a starting point for how IT auditors should manage their careers as they are impacted by green IT.

Changes in the IT Audit Universe

Green IT programs change the IT environment. Green initiatives such as cloud computing, virtualization, outsourcing, data center redesign and workstation management impact the components that IT auditors assess when performing audits. This raises two questions:

1. Should the audit universe for this year contain a green IT audit—an audit that evaluates IT green initiatives across the company?
2. Should green control objectives be added to each individual IT audit that is performed?

On the surface, these seem to be easy questions—that is, until one gets into the details of planning audits. For example, consider an organization pursuing a data center redesign to improve air circulation and decrease energy costs. Does the IT auditor visit the data center to audit the redesign only, and then return next month when performing the annual data center security and environmental controls audit? Or, should these trips be combined? There is no right answer to this question—each environment is different, but it is something that the IT auditor should think through.

This issue is exacerbated by political issues, timing and resource availability, as well. Some IT departments may be collaborative and actively seek involvement from IT audit on these initiatives. Others may be more closed and may suggest that the IT auditor’s scope be limited to...
Sarbanes-Oxley IT controls over financial reporting, which excludes green IT initiatives. The IT auditor must also address the continued downward pressure on budgets and resources. Everyone may agree wholeheartedly that audits should be expanded to include green IT, but IT audit resources may be stretched too thin to provide coverage.

**Recommendation**  
It is recommended that the IT auditor gain an understanding of what green IT activities are planned, underway or recently completed by the organization. This will provide a starting point for determining how the IT audit universe should change. By comparing those activities against planned IT audits, it should be clear how to react. Start by adding a few green IT audit procedures to the planned IT audits, or by requiring more comprehensive procedures or distinct audits. Significant projects that impact mission-critical systems should be considered as any other major implementation, and may require IT audit support throughout the duration of the project. By thinking through the impact on the IT audit universe in advance, IT auditing resources can be proactively managed more effectively.

**CHANGES IN AUDIT FINDINGS AND REPORTING**  
Green IT activities are changing the way the IT function operates. The progressive IT auditor understands these changes and modifies procedures and findings accordingly. Some green IT solutions appear incongruent with IT control objectives, or even mutually exclusive. For example, who can forget how many IT functions pursued high-availability strategies? The theory was sound: eliminate single points of failure by building in layers of redundancy throughout the IT environment. By doing so, the theory was that failure of any single device would not interrupt continuity of services. IT auditors were thrilled. This allowed them to finally close out those outstanding audit findings on disaster recovery planning.

Those redundancies now represent waste and overconsumption of electricity. Green IT initiatives may start to remove these redundancies, which will help achieve cost reduction and green IT goals, but put the IT auditor into a difficult situation—choosing between reporting these changes to management as “improvements” and “successes” or reporting them back as “deficiencies” and “audit issues.”

**Recommendation**  
The best way to address this conflict is to focus on straight talk. It is recommended to obtain the organization’s green IT strategy and project plan and review it in detail, paying close attention to items like consolidation, virtualization, environmental controls, and removal of IT applications or hardware. By understanding what is to be done under the banner of green IT, the IT auditor can proactively identify those green IT initiatives that may represent security or control issues, and have discussions with IT management before they occur.

In some cases, the IT audit function may not have visibility into these changes until after they occur, limiting the ability to influence decisions that may pose control issues. If so, IT auditors should operate with a heightened sense of awareness that objectives have changed, and new goals are taking priority. This requires an increased amount of diligence on the IT auditor’s part when it comes to validating findings and drafting reports. The IT auditor should seek to understand the IT department’s perspective and consider increased reporting timelines due to the need for additional discussions with the affected parties and reviews of audit reports.

**MORE OPPORTUNITIES TO ADD VALUE**  
IT auditors generally seek to add value to the enterprise through sound recommendations based on their audit results, or by bringing an IT controls and risk perspective and experience to IT initiatives. Opportunities to add value, however, can be few and far between, particularly when IT auditors are performing tests of the same Sarbanes-Oxley controls that have been tested annually since 2005 and are trying to get the testing done in 30 percent fewer hours this year.

Green IT is an opportunity for IT auditors to get reengaged in key business strategies and bring insight to the IT function that can translate to increased stakeholder value. For example, although many data centers were well planned when they were constructed, over time, equipment was acquired based on where it physically fit, as opposed to how it might help reduce the cooling needs of the data center. Oftentimes, a straightforward rearranging of the data center into alternating rows of cold and hot equipment can dramatically increase airflow, with a corresponding reduction in utility costs. This is not to say that such a rearranging is simple, but it generally does not require a large capital expenditure.
An IT auditor could also work with IT management to help develop a new green policy for workstations. Screen savers, for example, use more energy than putting a workstation into sleep mode. Energy settings on workstations, printer settings, orphan device management and other workstation default settings can have a big impact on energy consumption, while simultaneously increasing security and control.

Last, many organizations are looking for green achievements to publicize. IT auditors can provide leadership to assist with some of these initiatives for the organization. By doing so, they will not only help bring value to the organization, but they can also increase the visibility of their personal brand within the organization.

Recommendation
Bring ideas. Green IT is a growing field, and there is not a checklist for how to do it right. The opportunities for real savings are going to be driven by the specifics of each individual environment. In many organizations, IT auditors have greater knowledge of the broad IT environment than the IT staff members (who are solely focused on their areas of responsibility). Thus, the IT auditors can see opportunities that are missed by line management.

To bring ideas, IT auditors must continue to educate themselves and enhance their knowledge along a wide spectrum of information: hardware, processing units, HVAC ducting and airflow, tax subsidies and incentives (federal, state and local), building design software, etc. The IT auditor who takes the extra time to educate themselves along these lines will be able to continue delivering shareholder value and insight to the IT function and the organization.

CONCLUSION
Green IT initiatives are changing the way that organizations approach IT. This represents challenges and opportunities for IT auditors. It is an evolving field and those IT auditors who embrace it will receive career dividends, while those who do not may find themselves at odds with IT management. Think about how the organization’s IT environment is changing, and start evaluating how to help to reengineer aspects of one’s approach to auditing that environment.

AUTHOR’S NOTE
This article contains general information only and Deloitte and the author are not, by means of this article, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This article is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect the business. Before making any decision or taking any action that may affect the business, consult a qualified professional advisor.

Deloitte, its affiliates, and related entities shall not be responsible for any loss sustained by any person who relies on this article.
The Social Psychology of IT Security Auditing From the Auditee’s Vantage Point: Avoiding Cognitive Dissonance

Independence, objectivity and impartiality are all auditing hallmarks and are essential if an auditor is to render sound professional opinions that are constructive components of corporate governance and capital resource allocation judgments. Yet, they are all seemingly innocuous descriptive terms that are also chock-full of innuendos and dissonance. Perhaps an understanding of social psychologist Leon Festinger’s seminal research on his theory of cognitive dissonance would help. The theory examined the psychological phenomenon that presents discomfort when an individual is faced with a discrepancy between their existing beliefs and their actions. According to the cognitive dissonance theory, there is a tendency for individuals to seek consistency among their cognitions (i.e., beliefs, opinions) and actions. When there is an inconsistency between attitudes and behaviors (dissonance), something must change to eliminate the dissonance. In the IT context, dissonance occurs when an auditor perceives a logical contradiction among their cognitions and their professional code of ethics. ISACA’s Code of Professional Ethics for auditors states the following:

*Perform their duties with objectivity, due diligence and professional care, in accordance with professional standards and best practices.*

This article discusses the auditor’s objectivity and due diligence, as a corollary to requisite soft skills or the social psychology of conducting a security audit and the need to understand the individual’s (auditee) thoughts, feelings, behaviors and influences. Recognized principles of human social behavior hold the potential of teaching auditors some useful techniques to improve their auditing services.

Many information security specialists will agree that security depends on people more than policies, controls or technology.2 Extending this maxim, people (employees) pose a far greater threat to information security than outsiders.

It follows from these observations that improving security depends on changing beliefs, attitudes and behavior of both employees being audited and auditors. Social psychology can assist an auditor’s comprehension of how best to work with human predilections and predispositions to achieve their goals of improving security.

The social psychology issue of dissonance is brought to bear when an auditor’s independence and objectivity are impaired by preconceived notions or generalizations, which present as an issue of dissonance a possible conflict with the previously quoted statement of ISACA’s Code of Professional Ethics, which mandates objectivity, due diligence and professional care. Preconceived notions or generalizations arguably impair an auditor’s objectivity.

The aim of a security audit is to express an opinion based on an unbiased evaluation of the system in question after performing some test. Since time and resources are in short supply, the entire IT infrastructure cannot be tested; therefore, only a subset of the system is examined by an auditor, which may appear arbitrary to the auditee and objective to the auditor if their findings note issues of noncompliance with standards or IT security lapses.

Yet, the human psychology of the audit client (when collecting and evaluating evidence of an organization’s information systems, practices and operations) is often overlooked, with emphasis usually placed on the process and not the client. In a number of ways, auditing is a human relationship business. As such, auditors should understand the social psychology or the people side of auditing beyond the standards, procedures...
and best practices. Clearly, it is important to understand the process of obtaining and evaluating evidence to determine if an information system adequately safeguards assets and maintains data integrity while operating effectively and efficiently to achieve the organization's goals and objectives. However, understanding the social psychology of IT security auditing is equally important as the auditing processes and procedures. Doug Schweitzer, an Internet security specialist and freelance writer, stated:

“Security isn’t only about protecting your network from external threats; it’s also about protecting against threats from within. The first step to security is awareness; therefore, it’s important that all your employees know not only the potential threats but also how to recognize and prevent such threats. Education and awareness empowers each employee with the knowledge of his role in protecting the organization’s network. This, in turn, will go a long way toward mitigating risk.”

Persuading audit clients to become more security-conscious may involve finding ways to overcome auditing anxiety by effectively communicating with auditees, and letting them know what they are expected to do and what the auditor is doing to support their efforts to reasonably safeguard the organization’s information assets. However, no security controls or technology will successfully protect an organization if employees are naive, poorly trained or not made aware of the impact of security violations. Again, security depends on people more so than technology. Therefore, improving security depends on changing the beliefs, attitudes and the behavior of audit clients. Social psychology can help us better understand how to work with human predilections and predispositions to achieve the auditor’s goals of improving security.

COGNITIVE DISSONANCE THEORY
More than half a century ago, social psychologist Leon Festinger developed the cognitive dissonance theory. Cognitive dissonance is an uncomfortable feeling caused by holding two contradictory thoughts simultaneously. The thoughts or cognitions in question may include attitudes, beliefs and awareness of one’s behavior. The theory of cognitive dissonance proposes that people have a desire to reduce dissonance by changing their attitudes, beliefs and behaviors, or by justifying or rationalizing their attitudes, beliefs and behaviors.

Dissonance normally occurs when people perceive a logical inconsistency among their cognitions. This happens when one idea implies the opposite of another. For example, an auditor having a predisposition prior to the audit is inconsistent with ISACA’s Code of Professional Ethics. Becoming aware of the contradiction would lead to dissonance, which is characterized by a host of emotional states such as stress, anxiety, shame, guilt, anger and embarrassment. Audit clients may also experience dissonance when they smile and heartily agree to assist the auditor in any way possible; when in fact the auditee may feel that the auditor is:
- Simply overlooking what is being done right in order to find problems
- Blindly operating from an archaic set of laws and regulations that he/she knows are no longer relevant
- There to do management’s dirty work (i.e., get people fired)
- Not weighing the severity of the risk against the cost of containing or eliminating the risk
- Asking dim-witted questions
- Unaware of how the systems work, resulting in asking the same questions over and over again
- Asking for documents no one reads or has
- Wasting time getting documents and running meaningless test(s)
- Visiting only to find mistakes and report them to the boss
- Writing up harmless findings as if it will put the company at dire risk

Given the audit client’s feelings, information may be withheld, omitted or even hidden from the auditor. Such conflicting emotional distress may cause anxiety for the auditee and lead to rationalization (the tendency to create additional reasons or justifications to support one’s behavior).

Festinger’s cognitive dissonance theory is based on three fundamental assumptions (see figure 1):
1. Humans are sensitive to inconsistencies between actions and beliefs. Auditees may recognize at some level when their behavior is inconsistent with their beliefs, attitudes and opinions. In fact, one could argue that everyone has a built-in filter that alerts them when inconsistency between their actions and thoughts occurs.
2. Recognition of this inconsistency will cause dissonance and will motivate an individual to resolve the dissonance. When an auditee realizes he/she has violated one of his/her principles, some type of emotional anguish will occur. The degree of dissonance will vary based on the individual's level of conviction and the extent of inconsistency between behavior and actions. Motivation to resolve the perceived dissonance increases proportionately to the degree of dissonance.

3. Dissonance will be resolved in one of three basic ways:
   - Change beliefs—Perhaps the simplest way to resolve dissonance between actions and beliefs is simply to change beliefs. Fortunately or unfortunately, individuals’ basic beliefs and attitudes are fairly stable and are not likely to change easily unless they understand or perceive a reason for doing so. Although this option seems easy, it is infrequently embraced.
   - Change actions—A second option is cessation—never performing that action again. However, aversive conditioning (i.e., guilt/anxiety) often goes amiss. A problem with this option occurs when individuals rationalize away the negative feelings, thereby alleviating the need to change their actions.
   - Change perception of action—A third and more complex method of resolution is to change the way one views, remembers or perceives an action. That is to say, rationalization occurs. For example, auditees may justify stonewalling since an auditor is wasting their time anyway. Or they could say to themselves that everyone stonewalls the auditor, so why not us? By engaging in some mental gymnastics, auditees can reframe their actions in a different manner or context, so as to alter their views to align their beliefs with their actions. Such behavior is usually discernible on the part of others, yet difficult to detect in oneself.

SECURITY AWARENESS
A security awareness process that engages and educates the audit client can help better secure the organization's IT resources. A broad base of informed workers is a cost-effective way to mitigate security risks and better assist auditors. To change the audit client's negative perceptions, it is essential to have an understanding of behavioral patterns that are often at the core of misconceptions. An auditor should understand how audit clients:
   - Internally develop a system for assigning meaning to the ostensibly unrestrained control wielded by the auditor
   - Inadvertently distort their ability to understand and cooperatively facilitate the audit process due to their belief system
   - Due to misunderstandings, may act or react with the auditor in detrimental and unproductive ways that further exacerbate miscommunication and often lead to rationalization and generalization, which, in turn, yield more resistance

The often ignored objective of an audit is to build a sense of security awareness one user at a time. In fact, studies show that when people understand why they are being asked to do something, they are more inclined to cooperate. A case in point: When zoo signage was replaced from, “Please stand three feet from the cage” to, “Animals spit,” drastically different behavior was exemplified by the zoo patrons. Simply explaining why a safe standing distance was necessary had positive results. Prior to changing the signage, patrons would often be seen sitting or leaning over the safety rails, yet after understanding the reasoning behind the request, patrons stood well beyond three feet when viewing the animals. Changing the thoughts or beliefs of the zoo patrons ultimately changed their actions—which supports the cognitive dissonance theory.

Auditing was originally designed as a didactic profession that tended toward documenting findings focused on the mistakes and the negative behavior or practices of others. Historically, auditors would show up unannounced, conveying an implied message of surprise or distrust to the audit client, with the perception being that an auditor’s objective was to simply catch the auditee in the act of doing something wrong. Or, even worse, auditors would ask clients to make modifications or corrections because of some rule(s) without an adequate explanation.
To bring about security awareness, auditors must be willing to relinquish a measure of control, as they learn to facilitate risk reduction through effective communication. Once auditees are empowered to realize that they have the resources and authority to better safeguard the organization’s information assets, their actions will respond accordingly. An essential part of developing security awareness is to engage the auditee and allow the auditor to experience a paradigm shift—where auditors begin to comprehend the problems they unintentionally create by their mere presence.

CONCLUSION
The social psychology of security auditing from the auditee’s vantage point is paradoxical in that people are alike yet different. People are physiologically alike (eyes, ears, nose, mouth, mind, etc.) and share the same biological needs (air, water, food, clothing and shelter). Conversely, people are also uniquely different—emotionally, physically, mentally—with varying levels of motivation. Suffice it to say, maintaining a balance between treating everyone the same and being sensitive to individual differences is a challenge at best.

People bring their own perspective to the auditing process, which is colored by their predilections and predispositions. Auditors ought to realize on a human behavioral level that neither behaviors nor security conditions are static, with each constantly changing to meet the demands posed by new and changing security threats. Security perceptions are the predecessor to attitude formation and beliefs that subsequently shape security impression.6 Understanding the cognitive dissonance principle and applying some of the fundamental social cognition constructs or audit awareness will help auditors avoid auditing dissonance, which could impair the objectivity, due diligence and professional care that are required by ISACA’s professional ethics standards and best practices. The following summary is a listing based on well-established principles of social psychology. These tenets, in no particular order, identify ways an auditor can mitigate or avoid auditing dissonance by:7

- Participating in a security awareness effort, which includes many realistic examples of security requirements and breaches
- Endeavoring to inspire a commitment to security rather than merely describing it
- Emphasizing improvements rather than reduction of failure
- Listening with understanding for current security beliefs among employees and managers
- Never glorifying computer criminals with accolades or positive images and words
- Challenging employees who dismiss security concerns or flout security requirements; never ignoring such attitudes or beliefs
- Identifying senior executives most likely to succeed in setting a positive tone for subsequent security training
- Encouraging specific employees to take on public responsibility for information security within their work group
- Collaborating with management to build a culture that rewards responsible behavior such as reporting security violations
- Contributing to a working environment in which employees are respected. Explaining why IT security is important and the role each client plays in shoring up system security is more conducive to good security than operating in an environment that devalues and debases employees.
- Discussing security matters one on one with the participants, where possible, before calling a general meeting
- Remaining impartial and encouraging open debate during security meetings
- Bringing in outside experts as appropriate to counter groupthink and routinely playing devil’s advocate (taking the opposing viewpoint) during security meetings

ENDNOTES
1 ISACA, Code of Professional Ethics, www.isaca.org
4 Festinger, Leon; A Theory of Cognitive Dissonance, Stanford University Press, USA, 1957
5 Randolph, Alan; Getting the Job Done! Managing Project Teams and Task Forces for Success, Prentice Hall, USA, 1992
6 Op cit, Lippa
7 Ibid.
Access anywhere, anytime...

an abundance of knowledge on-demand.

**ISACA eLibrary** is a comprehensive online collection of content from nearly all ISACA/ITGI-published books and more than 400 third-party publications—all available **free of charge** as a benefit of your ISACA membership. It’s your own professional library available 24/7.

Check it out at [www.isaca.org/elibrary](http://www.isaca.org/elibrary).
IT Risk Analysis—The Missing “A”

An accurate assessment of IT risk is essential for the development of a relevant and cost-effective IT control environment. Unfortunately, the tools and conceptual framework for IT risk analysis have often included only highly visible metrics, such as number of transactions, direct financial impact, and the effectiveness of disaster recovery and business continuity across the enterprise. These traditional markers are important and valid in the assessment of risk. However, this article explores the concept that IT risk is also driven by a more abstract but potentially powerful factor: the organization’s level of commitment to agile systems. The term “agile” is used here in the strategic sense—as the ability to adapt quickly and efficiently to business, regulatory and technical changes.1

George Westerman and Richard Huntsman, in their book IT Risk,2 break IT risk into four categories: availability, access, accuracy and agility (the four “A’s”). While most IT audit risk analyses include the first three categories, agility is sometimes ignored in spite of its strategic importance to the ongoing success of the organization. Agility, the ability to respond appropriately to the organization’s business needs, is the most “fuzzy” of the four risk categories, but may be the most important from the perspective of day-to-day delivery of results.

TACTICAL VS. STRATEGIC RISK
The traditional focus of IT risk analysis has been on visible and tactical events. In terms of the Westerman-Huntsman model, those events include breakdowns in computing resource availability, inappropriate access and inaccurate processing. Of course, mitigation of these well-known risks is essential for the continuity of any organization. However, longer-term and slow-developing risks, such as the failure to maintain agile systems, can present significant harm to profitability and efficient operations. Agility risk is strategic and develops over time. It may not be immediately visible and, hence, may be more difficult to evaluate and present to management.

Agility directly affects the organization’s ability to respond to technical, regulatory and competitive market changes. Agility risk may...
come from lower-level, “nuts-and-bolts” factors or from improper strategic organizational structures. On the low end, for example, a legacy program might be written with hundreds of go-to statements. It may work perfectly well (after much debugging), but if it must be changed, the probability of failure is very high. Bad programming practices lead directly to nonagile systems. At the other end of the spectrum, an organization with high strategic agility risk may have siloed and disconnected applications, an excessive number of interorganizational links, and limited ability to change IT functionality within a reasonable time.

**WHEN CHANGE IS CONSTANT: THE STRATEGIC VALUE OF AGILITY**

In the 1990s, many progressive organizations implemented workflow systems as an important component of their business process management strategy. The benefits were and remain clear: structured movement of information with audit trails, straightforward authorization procedures and the ability to provide alternate paths if resources are temporarily not available. In an Oracle enterprise resource planning (ERP) system, for example, purchase orders flow from a lower-level initiator to a higher-level approver if the amount exceeds a predefined level, and other steps in the purchase-to-pay cycle follow. In a change control system, implementation of a program change cannot be put into production until a user/authorizer electronically approves the move.

In contrast, today’s for-profit and nonprofit businesses are increasingly compelled to go beyond the hierarchical, one-step-at-a-time processes tailored to workflow systems (although workflow systems continue to play a vital role in many core processes). In the marketplace, change is occurring at an exponentially increasing rate. Customers have the availability of the web, vastly more leverage than before and the flexibility to change providers easily. Hence, for many businesses, the ability to shift and be first to market is often more important than the capacity to produce cheap, standardized widgets. Product and service disruption is no longer an occasional event. Now disruption is nearly constant. Only agile firms can shift products, offerings, services and suppliers fast enough to maintain or increase market share. Increasingly, it is the nonroutine actions that drive competitive advantage. Thus, organizations with agile IT systems will thrive relative to other organizations when market conditions, governmental regulations, technology and other factors are the most disruptive.

**THE PATH TO AGILITY**

A strong, uniform, stable and predictable software platform may be the most essential element of an organization’s IT risk reduction program. And while a strong platform (software, hardware and methodologies) affects all areas of IT risk, it has a disproportionate effect on agility risk. Unfortunately, there is no simple formula for achieving the IT flexibility most firms need to respond to rapid change. Forward-thinking firms seeking to maximize agility encourage idea sharing, nonhierarchical decision making and full utilization of the entire organization’s mind space (including employees, contractors, vendors and customers). Such organizations often promote agility with human interaction tools.

Examples of these tools (mostly falling under the web 2.0 umbrella) include collaboration packages, information-sharing software (such as Microsoft’s SharePoint), wikis, blogs, alerting systems, hosted services for rapid change, social networks and even mashups. A number of organizations have used the spare cycles of millions of volunteer PCs to assist in problem-solving tasks. One example is the Folding@home project, which provides medical researchers with the equivalent of a massive supercomputer to solve difficult protein folding problems.

An organization without these capabilities runs the risk of delayed responsiveness to its customers and market conditions. In his book *Dot Cloud: The 21st Century Business Platform Built on Cloud Computing*, Peter Fingar notes that traditional companies are not only dramatically asymmetric in compensation, but also in availability of information. Workers may be uninformed about the business, unaware of the activities of other groups and unclear about the direction of the company. Top executives may (but not always) have access to vast amounts of detailed and summary data (e.g., business intelligence reports), whereas lower-level employees are often virtually in the dark. Organizations of the future must rely on crowd computing, taking advantage of the intelligence and knowledge of multiple groups, including employees, vendors, customers and others in relevant communities of interest.

**EXCESSIVE FOCUS ON VISIBLE RISKS**

There is an old joke about a partygoer who is hanging around a lamp post looking for his car keys. When asked why he is looking only in that one spot, he says, “it’s just common sense—the light is better there.” To a lesser extent, reviews of
enterprise risk have followed the same trajectory. Hurricanes, earthquakes, high-profile frauds and major accounting errors are visible. And while not everyone agrees on the particulars for a path to mitigation, there is at least consensus that, indeed, such events represent clear risks. For auditors, the lamp post light shining on highly visible risks is the brightest. Silent but corrosive agents of destruction may get overlooked because they are accretive and express themselves only over time. **Figure 1** illustrates the general relationship between categories of risk and their applicable time frames. Strategic risks, which may or may not be greater in magnitude than tactical risks, are less visible. Peter Weill and Jeanne Ross, in their book *IT Savvy*, note the effect when siloed, nonstandard and nonintegrated systems are proliferated:

Many IT professionals are quite adept at making disparate systems look integrated, but the code required to link applications becomes increasingly complex. Over time, key systems have so many links to other systems that even small changes are time-consuming, expensive and risky.

**Figure 1—Relative Time Frame for Risk Visibility**

The same lack of standardization mentioned previously can also be viewed from a platform perspective. If an organization commits scarce capital to developing specific IT capabilities, it needs to have assurance that the technological base or platform is stable and well defined. In the same sense that home builders need to work in a consistent metric—meters or feet—developers need assurance that the necessary technologies will be available and properly controlled so they can count on a set of capabilities. For example, assume an organization has a single, enterprisewide ERP system and needs to install a sales tax package, such as Vertex. If the new software requires a web services interface, all relevant applications can be linked to the package using the same interface. In contrast, for an organization with multiple ERP systems, installing the same package will require considerably more effort since multiple interfaces are needed. In addition, the risk of a sales tax calculation error increases with the number of unique interfaces required.

If IT auditors are to look beyond the standard three A’s of risk (availability, access and accuracy) and move into the realm of strategy (agility), the next question is—how? Traditional risk areas, such as disaster recovery and business continuity, are considered within scope of audit reviews. Looking at strategy is not as common. However, it is suggested as a direction of high payoff. In the next section, possible ways to introduce agility risk into the traditional availability portfolio of IT risk assessment are outlined.

**THE AUDITOR’S ROLE IN ASSESSING AGILITY RISK**

How do auditors use these concepts in their day-to-day work? Are strategic concerns only within the purview of senior management, or do they have a place in the auditors’ assessment of risk? In the past, perhaps they did not, but in the 21st century, organizational survival depends on agility. Its importance demands that it be included in any meaningful risk analysis.

Unfortunately, there is no canned prescription for the auditor’s review of agility risk. Certainly, there are IT functional bellwethers, pointing to the presence or absence of system flexibility, tool sets and appropriate information structures. **Figures 2 and 3** show example characteristics of organizations with low agility risk (desirable) and high agility risk (undesirable). These are suggestive only—real organizations vary so much that an “agility checklist” is not feasible or practical.

Auditors typically perform formal risk assessments to help develop annual audit plans. A weakness of many risk assessments is their reliance on a simplified model or a narrow perspective. For example, it is unlikely that a 1985
• New products, processes, geographic locations and acquired entities can be implemented without excessive cost, time or disruption to the rest of the organization or IT systems.
• Useful systems can be scaled and used by other divisions or subsidiaries without the risk of breakdown.
• Subsidiaries can be sold without undue cost of disposal.
• Systems are standards-based (e.g., for protocols, databases, middleware and other elements). New applications can be easily integrated into existing platforms.
• Development tools, database technologies, languages and other IT components are current, so that work can be outsourced if otherwise appropriate for the organization.
• Enterprisewide analytics, such as customer behavior summaries across all business units, can be readily obtained without unwieldy cross-reference tables or complex data extraction/reformatting over multiple systems.
• Software as a Service (SaaS) is used to provide off-the-shelf applications. For example, if an organization simply needs to pay its employees and does not use human resources/payroll to gain some strategic advantage over competitors, a generic package hosted and maintained by a third party may provide greater flexibility and possibly lower cost.
• Management is committed to the concept that new systems and changes to existing ones are made based on the long-term needs of the entire enterprise. Parochial systems and structures that do not integrate with other enterprise systems are discouraged. For example, multiple item numbers for the same physical product are not proliferated across multiple business units.
• An architecture of reusable software, algorithms and processes allows rapid but safe deployment of IT systems to meet immediate business needs. Service-oriented architecture (SOA) fits this model perfectly. However, even a partial implementation of the SOA concept speeds delivery by deploying pretested, shared computing components.
• A business model is used as the scaffolding for uniform IT systems. A bank, for example, will have a standard way to open a customer account, score credit, manage relationships across many products and so on. The model then translates into specific IT systems and processes that are uniform across the enterprise.
• Infrastructure is standardized, documented and properly architected to support business applications.
• Unstructured data (typically vital to rapid development) has a secure place in IT’s strategic architecture. For example, it is not left isolated on individual hard drives.
• IT systems have the ability to meet unforeseen customer actual demand, rather than merely matching forecasted demand. For example, factory production lines are linked to IT systems that are flexible enough to meet rapidly changing customer preferences.
• Rapid response/ flexible tools and methods are a part of IT’s tool kit. For example, virtualization, cloud and/or crowd computing may be used, allowing rapid increases or decreases in transactions, information flow, etc.

Risk analysis of threats to the profitability of Encyclopedia Britannica would have considered the negative sales impact of user-generated articles found on Wikipedia. The key to risk containment is not the ability to predict specific risks, but the agility to respond to unanticipated events, whether physical disasters, technology changes or simply fickle shifts in customer tastes.

For audit groups attempting to include more strategic concerns in their assessment of risk, including agility, one approach may be to start with specific projects. Rather than address enterprisewide IT agility risk all at once, pointing out “agility killing” practices for a new system in development may be an easier entry point. For example, if a nonstandard package is proposed as the solution, the auditor can ask questions such as:
• How will the data be integrated with the rest of the organization? Will interface routines need to be written?
• Can this package be easily modified if the business model changes?

Figure 2—Characteristics of Organizations With Low IT Agility Risk (Successful Management of Agility Risk)

<table>
<thead>
<tr>
<th>Characteristics</th>
</tr>
</thead>
<tbody>
<tr>
<td>New products, processes, geographic locations and acquired entities can be implemented without excessive cost, time or disruption to the rest of the organization or IT systems.</td>
</tr>
<tr>
<td>Useful systems can be scaled and used by other divisions or subsidiaries without the risk of breakdown.</td>
</tr>
<tr>
<td>Subsidiaries can be sold without undue cost of disposal.</td>
</tr>
<tr>
<td>Systems are standards-based (e.g., for protocols, databases, middleware and other elements). New applications can be easily integrated into existing platforms.</td>
</tr>
<tr>
<td>Development tools, database technologies, languages and other IT components are current, so that work can be outsourced if otherwise appropriate for the organization.</td>
</tr>
</tbody>
</table>

Figure 3—Characteristics of Organizations With High IT Agility Risk (Poor Management of Agility Risk)

<table>
<thead>
<tr>
<th>Characteristics</th>
</tr>
</thead>
<tbody>
<tr>
<td>Systems are not scalable and cannot accommodate rapid growth. For example, a warranty claim process may be written in Microsoft Access and, due to acquisitions, must now scale from 50 to 500 users. Platforms not designed to scale beyond a certain number of users become risky at the margins of their capacity.</td>
</tr>
<tr>
<td>The subsidiary’s links into corporate systems are convoluted and nonstandard. As a result, the cost to separate the subsidiary and corporate systems may be significant; it could influence the divestiture business decision.</td>
</tr>
<tr>
<td>Systems are not tied to the organization’s business model. Hence, the next acquisition represents a random and potentially permanent introduction of diverse databases, infrastructures, development environments, protocols and other technologies. High variability translates into higher IT costs and greater overall risk.</td>
</tr>
<tr>
<td>Vendor software is needlessly modified in unique ways by multiple business units within the organization. As a result, custom code proliferates more than is necessary, increasing the time, cost and risk when entitywide changes and new releases are implemented.</td>
</tr>
<tr>
<td>ERP systems are several releases out of date so that useful bolt-on packages cannot be installed without excessive cost and development time.</td>
</tr>
<tr>
<td>There is poor interim visibility of inventory, orders, etc., across the organization due to the heavy processing required to standardize data in disparate formats.</td>
</tr>
<tr>
<td>Application workflow is “hard coded.” New processes cannot be added without rewriting and extensive testing.</td>
</tr>
</tbody>
</table>
Can security be integrated into the existing security system(s), or will a separate security directory need to be maintained? For example, can the package use Windows Active Directory, or does a separate, duplicated user directory need to be maintained?

CONCLUSION
Many important factors in the life of large organizations cannot be quantified or can be quantified only in simple “yes/no” or “big/medium/small” terms. That does not mean that such factors are unimportant. For example, morale, enthusiasm for one’s work and job flexibility all strongly affect enterprise performance, but are hard to measure. Agility falls in that same camp. It is fuzzy but important. Auditors should include it in their assessment tool kit.

The pace of change in business and society demands that organizations maintain IT systems that are agile. The ability to quickly change products and services, divest and acquire subsidiaries without excessive effort, scale systems up and down, implement “loose coupling” of data transmissions, and link new social computing elements is critical. The auditor should include an assessment of agility as part of a strategic review of IT risk. Only the paranoid and agile survive.9

ENDNOTES
1 Use of the term “agile” in this article is conceptual and applies generally across the enterprise. It is not referring to the specific development life cycle technique referred to as “agile development.”
2 Westerman, George; Richard Hunter; IT Risk, Harvard Business School Press, USA, 2007
5 Peter Weill and Jeanne W. Ross, IT Savvy, Harvard Business Press, USA, 2009, p. 73-74
6 “Web services is a standards-based suite of technologies (XML, SOAP, WSDL, UDDI) designed to support interoperable applications to application interactions over a network.” Project Maui Glossary, University of Iowa, USA, http://provost.uiowa.edu/maui/Glossary.html, accessed 25 November 2009
7 According to Wikipedia News (http://en.wikinews.org/w/index.php?title=Encyclop%C3%A6dia_Britannica_fights_back_against_Wikipedia,_soon_to_let_users_edit_contents&oldid=780255, accessed 29 November 2009), “Encyclopedia Britannica, the authoritative reference book first published in 1768, is planning to let readers edit its entries, Jorge Cauz, its president said Friday, as it battles to keep pace with online Internet encyclopedia projects like Wikipedia.”
8 Loose coupling refers to the ability of systems to communicate with each other without rigid adherence to data layouts, sequencing of transactions and other highly idiosyncratic configurations. For example, the use of XML helps enable loose coupling because that protocol carries its own instructions on how the data are to be used. Minor program changes do not automatically result in changes to the interface structure.
9 A slight variation on the quote from Andy Grove, former chairman of Intel, “only the paranoid survive.”
By Myles Mellor
www.themecrosswords.com

1 Concern relating to data stored in a cloud
9 Sends a message to verify connection
10 The public domain standard for application management, abbr.
11 The ___ model of Plan and Organize, Acquire and Implement, Deliver and Support
12 Settle, a deal for example
13 Accounts receivable, briefly
14 Amount of work
15 Entry bar
16 Database component
17 Profit for short
18 Remote desktop, abbr.
19 Deceive
20 Contribute
21 Putting into practice
22 Premier global marketing intelligence company
23 Recommendation for professionals in relation to security: “Think like a ____.”
24 Software program for doing a task
25 Question for an IT auditor to ask on each risk identified to identify the impact of it
26 Put money into
27 Compass point
28 Publisher of Security, Audit and Control Features Oracle Database, 3rd Edition
29 Public domain standard for IT service procurement, abbr.
30 Publishe___
31 They created the BlackBerry.
32 Profit for short
33 It's good to be able to think out of it
34 Sundial number
35 Dulles Airport city
36 Internet laughter
37 Yes in Spain
38 Dulles Airport city
39 Dulles Airport city
40 Dulles Airport city
41 Dulles Airport city
42 Dulles Airport city
43 Dulles Airport city
44 Dulles Airport city
45 Dulles Airport city
46 Dulles Airport city
47 Dulles Airport city
48 Dulles Airport city
49 Dulles Airport city

DOwn
1 Ability to duplicate across different sites
2 One aspect when considering the risks related to IaaS
3 ____Basic: programming language
4 Predict, in a way
5 Reviewing how and when these are issued and for what would be a part of SaaS risk management auditing
6 Entry bar
7 Database component
8 Halt
9 Profit for short
10 Remote desktop, abbr.
11 Deceive
12 Contribute
13 Cost reductions
14 Retain
15 Putting into practice
16 Compass point
17 Software program for doing a task
18 Publisher of Security, Audit and Control Features Oracle Database, 3rd Edition
19 Public domain standard for IT service procurement, abbr.
20 They created the BlackBerry.
21 It's good to be able to think out of it
22 Sundial number
23 Dulles Airport city
24 Dulles Airport city
25 Dulles Airport city
26 Dulles Airport city
27 Dulles Airport city
28 Dulles Airport city
29 Dulles Airport city
30 Dulles Airport city
31 Dulles Airport city
32 Dulles Airport city
33 Dulles Airport city
34 Dulles Airport city
35 Dulles Airport city
36 Dulles Airport city
37 Dulles Airport city
38 Dulles Airport city
39 Dulles Airport city
40 Dulles Airport city
41 Dulles Airport city
42 Dulles Airport city
43 Dulles Airport city
44 Dulles Airport city
45 Dulles Airport city
46 Dulles Airport city
47 Dulles Airport city
48 Dulles Airport city
49 Dulles Airport city

(Answers on page 58)
Prepare for the 2010 CISM Exams

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

To pass the Certified Information Security Manager® (CISM®) 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/cismreview

to order CISM review material for the June/December 2010 exams, visit the ISACA web site at www.isaca.org/cismbooks or see pages S1-S8 in this Journal.

CISM Review Manual 2010 ISACA

The CISM® 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

CISM Review Questions, Answers & Explanations Manual 2009 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

2010 Editions
CQA-10ES English Edition
CQA-10JS Japanese Edition
CQA-10SS Spanish Edition

2009 Editions
CQA-9ES English Edition
CQA-9JS Japanese Edition
CQA-9SS 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

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
How does a service level agreement (SLA) for Voice-over IP (VoIP) telephony differ from any other standard SLA? My team is planning to conduct an audit on the VoIP project implemented recently. What are the specific metrics that the SLA should aim to measure in the context of VoIP telephony?

We can look at two different SLAs here: one between your company and the telecom service provider or Internet service provider, and also the one between your internal voice/telephone function and other business functions. I am not sure from your question which one you are keen to discuss, as both the business needs and users’ expectations dictate SLA metrics.

SLA metrics for VoIP can be categorized into the following four types:

- Call quality
- Call setup performance
- Availability
- Incident management

**CALL QUALITY**

As someone mentioned in one of the recent conferences I attended, there is a consumer within every user whose expectation as the corporate user is equivalent to that of the average consumer on the street. The chief technology officer (CTO) of a leading IT services provider lamented to me that someone who uses a web-based backup service demands, at the click of a button, the same in a corporate environment, not understanding and appreciating the constraints of a typical IT function. People who use VoIP expect the same level of call quality they would have using normal public switched telephone network (PSTN) lines.

Call quality in a VoIP context is measured using a unit called mean open score (MOS), which measures users’ perception on call quality. MOS is a metric to distinguish good calls from bad ones. On a scale of 1.0 to 5.0, an MOS score of 4.0 is considered equivalent to PSTN call quality and 3.6 and above can be deemed acceptable. Anything below a 3.6 MOS should be deemed as unacceptable in a typical business environment. Of course, tools are required to continuously monitor the call performance data, and the MOS value has to be computed. Network performance metrics such as jitter, lost packets and delay are used to derive MOS scores. It is pertinent to note that ‘codec’ is the fourth metric used to compute MOS, which is not measured on a real-time basis, but is usually measured as a fixed parameter on a per-call basis.

Your SLA should have clear metrics defined in terms of MOS scores. If VoIP is very critical to your day-to-day business operations, you can and must set higher/lower thresholds of acceptability. For example, you can even set anything below 3.0 MOS as unacceptable, while the industry norm is typically 3.6 MOS.

**CALL SETUP PERFORMANCE**

Once a VoIP call gets initiated, a series of events is expected to be triggered in sequence, without any errors. Call setup refers to the first of the series of events that get triggered. In a call setup phase, the following activities happen:

- Acquisition of dial tone
- Dialing out the destination phone number
- Obtaining the signal, be it a ringing tone at the desired destination or a busy tone
- Call setup response time—The time elapsed from the moment the phone is picked up until the dial tone is heard. If the delay is long enough—ideally, it should be seamless—users may think that the dial tone is not available and may hang up without making the call.
- Call setup response time—Relates to the quantum of delay between dialing out the destination phone number and when the ring tone or the busy tone is heard. It is also called as ‘post dial delay’.
Different call setup protocols are used—H.323, SIP, MEGACO, MGCP—in various VoIP implementations and any of them could lead to poor performance. These protocols operate using the TCP/IP protocol, sending a large number of different packets between the VoIP phones and the VoIP servers to establish the call between the source and the destination. Any lost or misdirected packet can lead to an issue.

**AVAILABILITY**
Availability, as the name implies, relates to the availability of the VoIP system in order for the users to make the calls as and when they need them. It goes without saying that the VoIP applications and systems must have disaster recovery and contingency arrangements in place, if the VoIP is deemed as a key business-critical service. In a normal PSTN environment, the users expect to hear the dial tone 99.99 percent of the time and also expect the call to go through and get completed without any disturbances and interruptions.

Availability metrics do not simply relate to the ‘downtime’ of the applications and systems. They include other components such as percentage of call completions, percentage of abnormal disconnections, number of busy call attempts caused by excess demand and limited supply of resources, and so on. It is essential that such metrics get captured and measured.

**INCIDENT MANAGEMENT**
It is very important that an incident management system be put in place to track, monitor and close incidents. Incidents can relate to availability or confidentiality risks. For example, information on who made the call, who was called, etc., can be deemed as private information in some jurisdictions. Call detail records (CDR) in a VoIP system must remain confidential, and access to the same must be provided on a need-only basis.

Any event that can evolve to an incident, crisis or disaster must be manageable; processes and controls must be in place to handle them, should they happen. Typically, mean time to repair (MTTR) and mean time between failures (MTBF) are used to track incidents.

**SUMMARY**
Thus, these four categories describe the key attributes to a VoIP SLA. It is needless to mention that other components such as the following must also find their place as with any other SLA for typical business-critical services:
- Reporting and frequency
- Ownership at both ends
- Governance
- Other relevant metrics
- Penalty on SLA violations
- Service credits, if any
- Periodic review
- Regular audits

An SLA is relevant and valid only when it is put in practice in the field. IT/voice services management must make it a live document by ensuring the publication of relevant metrics, followed by appropriate remedial actions, where necessary. The SLA must also be reviewed on a periodic basis to ensure its relevance, adequacy and appropriateness.
Quiz #130
Based on Volume 1, 2010—Risk Management and Assessment
Value—1 Hour of CISA/CISM Continuing Professional Education (CPE) Credit

TRUE OR FALSE

SUAN ARTICLE
1. In traditional business continuity planning, the physical and IT infrastructure are assumed to be intact; the only threat is in losing a large group of key personnel and key business supplies.
2. In the World Health Organization (WHO)'s six-phase framework, levels 1-3 indicate the need for response and mitigation efforts, and 4-6 indicate the need for capacity development and response planning activities.
3. Splitting key personnel into different workplaces reduces the risk of mass infection should one workplace be infected.
4. In a worldwide epidemic, a global shortage of critical supplies is likely as supply chains may be hampered by the pandemic.

SCHMITTLING AND MUNNS ARTICLE
5. Two primary examples of an enterprise risk approach requiring a periodic risk assessment are the US Sarbanes-Oxley Act and the US Health Insurance Portability and Accountability Act (HIPAA).
6. The rationale for performing an enterprise risk assessment includes breaking barriers and self-analysis.
7. A comprehensive risk assessment should be carried out at least once every five years to explore the risks associated with the organization’s information systems.

RAVAL ARTICLE
8. Gartner predicts that the market for cloud products and services will vault from US $4 billion in 2008 to US $160 billion in 2013.
9. The following four logical characteristics are evident in cloud computing: sharing, bandwidth, diversity and management.
10. The single most critical concern related to cloud computing is the authentication of users of web-based services.
11. An area of concern related to cloud computing is ownership of content.

SINGH AND LILJA ARTICLE
13. GRC platforms provide a single, federated framework that integrates organizational processes and tools, supporting those processes for the purpose of defining, maintaining and monitoring GRC.
14. When evaluating GRC vendors, it is not necessary to consider the total cost of ownership (TCO) as this has no impact on ROI.

SOLLIS ARTICLE
15. An example of the fallout of deficient internal controls is when 80,000 Macy’s customers were debited up to four times for a single transaction during a recent holiday season.
16. Manual processes that once worked can no longer keep up with the volume, pace and complexity of information.
17. Automated information controls add tremendous value to a business because they ensure the integrity of critical information and processes.
Quiz #130 Answer Form

(Please print or type)

Name _____________________________________________
__________________________________________________
__________________________________________________
__________________________________________________
Address __________________________________________
__________________________________________________
__________________________________________________
CISA, CISM or CGEIT# _______________________________

Quiz #130

True or False

SUAN ARTICLE
1. __________
2. __________
3. __________
4. __________

SCHMITTLING AND MUNNS ARTICLE
5. __________
6. __________
7. __________

RAVAL ARTICLE
8. __________
9. __________
10. __________
11. __________

SINGH AND LILJA ARTICLE
12. __________
13. __________
14. __________

SOLLIS ARTICLE
15. __________
16. __________
17. __________

Answers—Crossword by Myles Mellor

See page 53 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.
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 is 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 emphasizes 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](http://www.isaca.org/cobit).

Links to current guidance are posted on the standards page, [www.isaca.org/standards](http://www.isaca.org/standards).
Leaders and Supporters

Editor
Jane Seago

Senior Editorial Manager
Jennifer Hajigeorgiou

Contributing Editors
Sally Chan, CMA, ACIS, PAdmin
Kamal Khan, CISA, CISSP, CITP, MBCS
A Rafee, CISA, CGEIT, CIA, CQA, CFCA
Steven J. Ross, CISA, CBCP, CISSP
Tommie Singleton, Ph.D., CISA, CMA, CPA, CITP
B. Ganapathi Subramaniam, CISA, CIA, CISSP, SSCP, CCNA, CCISA, BS 7799 LA

Advising
The YGS Group
advertising@isaca.org

Media Relations
news@isaca.org

Editorial Reviewers
Matt Altman, CISA, CISAM, CGEIT
Linda Betz
Pascal A. Bizarro, CISA
Jerome Capirossi, CISA
Cassandra Chasnis, CISA
Ashwin K Chaudhary, CISA, CISAM, CGEIT
Joao Coelho, CISA, CGEIT
Reynaldo J de la Fuente, CISA, CISAM, CGEIT
Christos Dimitriadis, Ph.D., CISA, CISAM
Ken Doughty, CISA, CBCP
Adam Ely, CISA
Anuj Goel, Ph.D., CISA, CGEIT, CISSP
Manish Gupta, CISA, CISAM, CISSP
Jeffrey Hare, CISA, CPA, CIA
Francisco Igual, CISA, CGEIT, CISSP
KK Lim, CISAM
Romulo Lomparte, CISA, CGEIT
Juan Macias
David Earl Mills, CISA, CGEIT, MCSE
Robert Moeller, CISA, CISSP, CPA, CSQE
Aureo Monteiro Tavares Da Silva, CISAM, CGEIT
Gretchen Myers, CISSP
Daniel Paula, CISA, CISSP, PMP
PaK-Lok Poon, Ph.D., CISA, CSQA, MIEEE
John Pouey, CISA, CISAM, CIA
Steve Prinost, CISAM
Panvathi Ramesh, CISA, CA
David Ramirez
Ron Roy, CISA, CRP
Kalidasan Shanmugakani, CISA, CISSP
Johannes Tekle, CISA, CIA, CFSA
Ellis Wong, CISA, CFCA, CISSP

ISACA Board of Directors (2009-2010):

International President
Emil G. D’Angelo, CISA, CISAM

Vice President
George Ataya, CISA, CISAM, CGEIT, CISSP

Vice President
Yonosuke Harada, CISA, CISAM, CGEIT, CAIS

Vice President
Ria T. Lucas, CISA, CGEIT

Vice President
Jose Angel Pena Ibarra, CGEIT

Vice President
Robert E. Stroud, CGEIT

Vice President
Kenneth L. Vander Wal, CISA, CPA

Vice President
Ron M. von Roessing, CISA, CISM

Past International President, 2007-2009
Lynn Lawton, CISA, FBCS CITP, CPA, FIlla

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