

## INTERNAL AUDIT SOFTWARE

- ✓ Streamline the audit process
- ✓ Improve audit visibility
- ✓ Increase audit efficiency & productivity
- ✓ Leverage assessments by other GRC groups

■ **SAVE TIME, CONDUCT BETTER AUDITS**

## INTERNAL AUDIT SOFTWARE • THINK PAISLEY

Internal audit software from Paisley includes features for risk assessment, planning, scheduling, workpapers, reporting, issue tracking, time and expenses, quality assurance and personnel records. It is part of a comprehensive governance, risk and compliance solution that also includes functionality for financial controls management, compliance, risk management and IT governance.

Join over 1,300 leading organizations that utilize software from Paisley to increase efficiencies, reduce costs and improve the overall quality of financial, IT and operational audits.



**PAISLEY ENTERPRISE GRC™ AND GRC ON DEMAND™** — Software for integrated audit, operational risk management, financial controls management, IT governance, and compliance. **Call 888-288-0283 or visit [www.paisley.com](http://www.paisley.com)**

# Information Systems Control JOURNAL

The Magazine for IT Governance Professionals

VOLUME 3, 2008

## Columns

**5**  
Guest Editorial: Mobility Changes  
(Almost) Everything!

By William C. Boni, CISM

**9**  
IS Security Matters: Resilience  
Transformation

By Steven J. Ross, CISA, CBCP, CISSP

**11**  
IT Audit Basics: Beyond the IT  
in IT Audit

By Tommie Singleton, Ph.D., CISA, CITP,  
CMA, CPA

**14**  
IT Governance: IT Governance Global  
Status Report 2008: An Excerpt

By Dirk Steuperaert, CISA

**18**  
IT Value: Recognising the Need for  
Val IT: Identifying Tipping Points for  
Value Management

By Sarah Harries and Peter Harrison,  
FCPA

**20**  
Five Questions With...

Luis Eduardo Toro Lobos, CISM

## Features

**24**  
Book Review: Stepping Through the  
InfoSec Program

Review by C. Warren Axelrod, Ph.D.,  
CISM, CISSP

**25**  
Book Review: Information Development:  
Managing Your Documentation Projects,  
Portfolio, and People

Reviewed by Soumen Chatterjee

**27**  
A Prelude to IT Assurance Framework

By Ravi Muthukrishnan, CISA, CISM, FCA

**31**  
Using COBIT 4.1 to Guide the Adoption  
and Implementation of Open Source  
Software

By Steven De Haes, Ph.D., Wim Van  
Grembergen, Ph.D., Kris Ven and  
Jan Verelst

**37**  
Keys to Data Governance Success:  
Teamwork and an Iterative Approach

By Marty Moseley

**40**  
Case Study: Auditor Ethics for  
Continuous Auditing and Continuous  
Monitoring

By Jill Joseph Daigle, CISA, CIA, CISSP,  
Ronald J. Daigle, Ph.D., CPA, and  
James C. Lampe, Ph.D., CPA

**45**  
Computer-assisted Audit Techniques:  
Value of Data Mining for Corporate  
Auditors

By John Ott, CISA, CPA, Andrew  
MacLeod, CISA, CIA, FCPA, MACS, PCP,  
and Kevin Mar Fan, CISA, CA

**49**  
Pay Today or Pay Later—Calculating ROI  
to Justify Information Security  
and Compliance Budgets

By Jaspreet Singh, CISA, MCSE, MCSA,  
BS 7799 LA

**51**  
A Business Model for Information  
Security

By Kent Anderson, CISM

**53**  
Virtual Appliances—The Evolution of a  
Gold Standard

By Ronan Kavanagh

## Plus

**17**  
Standards, Statements, Guidelines  
ISACA® Member and Certification  
Holder Compliance

**57**  
Help Source Q&A  
By Gan Subramaniam, CISA, CIA,  
CISSP, SSCP, CCNA, CCSA,  
BS 7799 LA

**59**  
CPE Quiz #118  
Based on Volume 1, 2008  
By Kamal Khan, CISA, CISSP, MBCS

**S1-S8**  
ISACA Bookstore Price List Supplement

The *Information Systems Control 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 governance, control, security and assurance.



3701 Algonquin Road, Suite 1010  
Rolling Meadows, Illinois 60008 USA  
Telephone +1.847.253.1545  
Fax +1.847.253.1443  
[www.isaca.org](http://www.isaca.org)

Please fill out the reader survey  
at [www.isaca.org/readersurvey](http://www.isaca.org/readersurvey)  
to help us continue to improve  
the *Journal* to better serve  
our readers.

## Online

### Online Features

The following articles will be available to ISACA members online on 2 June 2008.

The Art of Database Monitoring 🌟  
By Sushila Nair, CISA, CISSP, BS 7799 LA

Billing Audit on a Mobile Operator—  
Call Detail Record 🌟  
By Dale Johnstone and Ellis Chung Yee Wong,  
CISA, CFE, CISSP

Role Engineering: The Cornerstone of RBAC 🌟  
By Srinivasan Vanamali, CISA, CISSP

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, including 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](http://www.isaca.org/journalonline).



The Leading Global Provider of Audit Analytics Technology

Chief Audit  
Executive

Internal Auditor

Technical Audit  
Specialist

Audit Team  
Manager

## Introducing ACL AuditExchange

### A Managed Analytics Platform for the Entire Team

ACL AuditExchange provides a secure and centralized environment for the whole audit team to access data, analyze business transactions and report on audit findings and results. Regardless of source and size, you'll have access to any type of enterprise data you need. With ACL AuditExchange you'll be able to create a central audit repository to capture and preserve audit knowledge and results. So, even when people leave, the remaining audit team can continue to efficiently produce consistent, high quality audits.

For 20 years, ACL has been the leading provider of audit technology. Visit [www.acl.com/AuditExchange](http://www.acl.com/AuditExchange) today for more information on how our latest innovation can help your team:

- Increase productivity by automating audit tests and sharing findings and results
- Share an audit repository across your team, wherever they are
- Improve access to any type of enterprise data

» Find out more at [www.acl.com/AuditExchange](http://www.acl.com/AuditExchange)

# fraud

## Don't let fraud go undetected.

# IDEA

## See it right the first time.

The analysis of company data is the single most effective way of detecting fraud. **IDEA** is the most powerful and complete *data analysis software* available today to assist you in the detection of fraud.

Auditors and fraud investigators in over 90 countries in 13 languages, use **IDEA** to outperform the expectations of clients, employers and regulators. For more information about **IDEA** and to request a free demo version, visit our website at [www.caseware-idea.com/new](http://www.caseware-idea.com/new).

### Streamline your data analysis with IDEA Smart Analyzer.

**IDEA Smart Analyzer** is an add-on collection of preprogrammed audit tests and reports that can be run by any auditor with a minimum amount of training. To download a 30-day evaluation version go to [www.caseware-idea.com/smartanalyzer](http://www.caseware-idea.com/smartanalyzer).



IDEA is a registered trademark of CaseWare IDEA Inc.

IDEA significantly improves your ability to detect fraud.



**William C. Boni, CISM** has spent his entire professional career as an information protection specialist and has assisted major organizations in both the public and private sectors. For more than 30 years, beginning as a special agent in US Army counterintelligence, Boni has helped a variety of organizations design and implement cost-effective programs to protect both tangible and intangible assets. In a wide range of assignments, he has assisted clients in safeguarding their digital assets, especially their key intellectual property, against the many threats arising from the Internet. He joined Motorola in 2000 to become its first corporate information security officer and corporate vice president of IT and security. Boni has served on the ISACA Board of Directors and chaired the IT Governance Committee.

# Guest Editorial

Industry leaders examine  
the latest business issues

## Mobility Changes (Almost) Everything!

Spring time in North America is a great time to reflect upon the many new challenges that are facing those in the security, audit and control professions. It seems that we are past the era when highly visible and disruptive, fast-spreading computer viruses and worms caused information security professionals hours of lost sleep and endless angst about the next attack. However, the relative calm of the present, even though punctuated by the all-too-frequent announcements of privacy breaches, is a deceptive quiet.

During the 30-plus years I have been working as an information protection specialist, I have never seen a time when we have faced such an imposing array of challenges that all seem to have coalesced simultaneously to confound our best intentions and subvert our good work. There are many factors contributing to this challenge, but I believe there are three major trends that are creating a new risk matrix that will challenge us all.

First, the convergence of ubiquitous connectivity and evermore powerful portable and handheld devices has resulted in a vast increase in fully mobile users. Fueling this rapid growth are new applications that are quickly making the old paradigms around network security anachronistic and ineffective. The notion of treating an organization's network as if it is a discrete environment and developing security solutions to guard against the threat of outsiders is dangerously outmoded and an incomplete concept.

We need to understand that this pernicious and outdated concept still affects our approach to protection, and many people continue to operate as if physical location is a reliable measure for protecting organizations against risks of information theft or loss. As we equip more of the workforce with smart phones, they become less tethered to predefined locales and, thus, create an expanding boundary for us to address. The "little laptops" now attached to belt loops or in pockets and purses are rapidly gaining both increased processing power and, more important,

new access pathways through third generation (3G) and fourth generation (4G), as well as WiFi and WiMAX, networks. Compounding the challenge is the parallel need to accommodate an ever-growing and frequently changing pool of temporary, contract and outsourced providers for many essential business services. So who is an "outsider" and who is the "insider" under these various arrangements? How would we define the boundary or perimeter of a network under this new paradigm?

These devices and applications/capabilities that are seeping into enterprises and more organizational content—some of it subject to legal, regulatory and contractual controls—have begun to migrate outside the classic network perimeter. As key content is pushed to mobile devices, the capability to secure all possible end points and the myriad access pathways becomes evermore difficult. Thus, the change in where people work (now anywhere they can obtain network connectivity) renders moot the concept that physical location is an acceptable factor for determining "insider" or "outsider" as a basis for controlling and protecting the organization's interest in a network and associated proprietary or private content.

The problems arising from this first trend are exacerbated by the so-called "consumerization of information technology (IT)," which I believe is the second trend we need to consider. In a thought-provoking article from the *Financial Times* published in December 2005, titled "The Future Ends at the Firewall," Richard Waters advised readers that often the best way to experience the full fruits of rapidly developing technology is to simply stay home! With high-speed Internet connections and a market of billions of users, the pace of innovation achieved by the consumer marketplace is breathtaking. Even a well-resourced IT organization is hard pressed to offer the variety and capability of solutions that can be downloaded with a mouse click at any residence with high-speed Internet access. Worse, at work most IT organizations



impose strict controls over users' workstations and limit the choice of applications, claiming "security" (what some pundits have called "Software Stalinism") requires these controls. Under these circumstances, there is no chance that innovation will trump protection, but before we become too smug about the "benefits" of such safeguards, we should consider the unintended adverse consequences that can arise from this common approach to "protecting our users."

The problem with the forced-controls paradigm is it runs directly counter to much of the value-creation model of the 21<sup>st</sup> century economy. Increasingly, new products, services and solutions require near-constant innovation. Innovation in a global community—the creative spark that envisions new experiences, products or services creation—comes as often from the *ad hoc*, unstructured, interpersonal and interorganizational discussion, as it does from formal research initiatives. When there is an idea that has potential, these initial communications must quickly evolve into full-blown collaboration. If "baroque"

network security architectures and policies do not accommodate and enable an innovation culture, then they risk imprisoning the creative staff in a sterile shell of controls that stifle agility and productivity gains, which may ultimately leave the organization uncompetitive in the global market.

You may think this is overstating the case, and I admit to dramatizing the situation to challenge the conventional wisdom. Many protection professionals seem so intent on childproofing work spaces to prevent risks that they underestimate the importance of creating controls and structures that also enable innovation, which is essential in today's fast-moving environment.

The first two trends, when combined, amplify the consequences of the third and perhaps most serious trend. Internet-connected organizations are being attacked by cybercriminals and cyberspies. Recent media reports in Europe, Asia and North America document a clear trend toward increasing frequency, sophistication and consequence of attacks targeting financially valuable proprietary, personal, operational and defense-related information. It appears some of the attacks are supported by organized criminal groups, some by Internet-enabled flash mobs responding to a *cause celebre*, and others may be state-sponsored by military or intelligence services of nation states. Where, in the past, threats often manifested themselves as attacks from curious or thrill-seeking hackers, the recent trend has shown the new generation of threats to be sourced from well-funded and organized adversaries, focused on financial gain or specific information targets.

While the value of digital mechanisms that enable interpersonal collaboration and communications cannot be denied, this value comes with some consequence. Increasingly savvy cybercriminals/cyberspies can exploit these collaborative environments virtually unnoticed by unprepared users and organizations. In the late 20<sup>th</sup> century, hackers seemed intent on maximum visibility for their actions. Conversely, in the 21<sup>st</sup> century, hackers seem bent on ways of parasitic extraction of value from targeted organizations that raise the least amount of concern and, thus, reaction from the "hosts."

As information security, audit and governance professionals, we must ask ourselves and challenge our organizations to effectively address these compelling risks. We must see that mobility has created a nearly perfect storm affecting information protection. We have new platforms that allow more organization data to be accessed and pushed outside the old perimeter firewall and, at the same time, the Darwinian struggle for survival in the global marketplace for value creation requires the ability to operate as an innovation engine—demanding greater access and collaboration. At the same time, threat actors have gone from being late 20<sup>th</sup> century hooligans, to organized and supported criminals or operatives!

The simple fact is, despite the best intentions of our professionals, we appear to be protecting the wrong things, using obsolete and largely ineffective tools that create at least as much harm as good. This misalignment between what we think and intend, and what we actually achieve, arises from a lack of integration of security/protection efforts, with full consideration of the broader organizational objectives and changes in the external environment.

I wish the solution was as simple as some new technology. The truth is, we must understand there are no "silver bullets" that will instantly neutralize these new risks, and spending more on security tools, if they are misaligned and not adapted, will fail. Technology, although part of an effective solution, is necessary, but insufficient.

I believe a more holistic approach to managing information risks that covers the full set of issues introduced by mobility, without stifling the innovation critical to value creation, is needed. We must find a balance among policy, process, awareness and technology that will stabilize demands for legal, regulatory and contractual compliance. Moreover, to enable the organizations we serve to be as productive as possible in achieving their missions, this balance must support innovation and creativity. If we fail to find this balance, then the cybercriminals/operatives will likely thrive, while the organizations we support are at risk of withering away due to their failure to adapt.

---

*We appear to be protecting  
the wrong things.*

---

## 36<sup>th</sup> Annual International Conference

27-30 July 2008

Sheraton Centre Toronto  
Toronto, Ontario, Canada



**ISACA's International Conference** is recognized throughout the world for its in-depth coverage of leading-edge technical and managerial issues facing IT governance, control, security, audit and assurance professionals.

A cadre of world-class presenters will showcase the differing ways in which similar problems are solved around the globe. Join us for a chance to participate in this global forum of IT leaders, and earn up to **40 CPE credits**.


### Conference Streams:

- IT Governance
- IT Audit Practices
- Information Security Management
- IT Risk Management and Compliance

Register online now!

[www.isaca.org/international](http://www.isaca.org/international)





Do you know which  
one of your team  
accessed your key  
financials last night?

**With Cyber-Ark® you will.**

With Cyber-Ark's Digital Vault Solutions, you will know **who** is doing **what** with your highly sensitive information, processes and systems and you will be able to **prove** it.

Does your enterprise's approach to risk management fully address the challenges around all of your privileged users and most highly sensitive data? Are you sure? Can you prove it?

For instance -- do you know who accessed your key financial systems anonymously as the System Administrator last night? Do you know who has the rights to both create and approve a purchase order? Or a speculative financial trade? Are you willing to risk your brand on the integrity of faceless insiders with privileged access to highly sensitive systems, information and processes?

With Cyber-Ark's suite of Digital Vault Solutions, you will always know that your most sensitive systems and information are secure, controlled, and completely managed in a provable, auditable manner.

Cyber-Ark's Enterprise Password Vault™ today enables over 300 global enterprises to address their Privileged Identity Management challenges. With the EPV as a core part of their infrastructure, enterprises can now:

- Manage, Personalize and Audit the full range of Privileged Users, including Administrative and Application Identities

- Automate manual processes and reduce IT's workload while serving the overall security and compliance goals

Coupled with the powerful Inter-Business Vault® and Sensitive Document Vault™ that create Communities of Trust for securely storing and sharing highly sensitive information within your organization and with your business partners, Cyber-Ark's suite of integrated Digital Vault solutions provides a solid, sustainable and robust solution to address any concerns around Privileged users and Highly sensitive information raised in SOX, PCI, Basel II, HIPAA and other regulations and IT frameworks.

So if your organization needs to know the who, what, where and when, then come and talk to us. After all the last thing your business needs is "15 minutes of fame".

**For further information on Cyber-Ark's  
Digital Vault solutions visit  
[www.cyber-ark.com/ISACA108](http://www.cyber-ark.com/ISACA108)  
or call Cyber-Ark Software on  
888 808 9005**



The Leader in Privileged Identity Management Solutions





## Resilience Transformation

By Steven J. Ross, CISA, CBCP, CISSP

I have written about resilience a number of times in this space, most recently in the last issue of the *Journal*.<sup>1</sup> I am finding that many companies perceive extended inability to serve their markets in a time of exceptional volatility to be their greatest security risk. By implication, there are aspects of businesses I encounter that are not resilient,<sup>2</sup> but their management would like to make them so. Most often, information technology (IT) resilience is at issue, but recent concerns about the possibility of a human pandemic have also raised concerns about the resilience of companies' workforces. Resilience and robustness have long been topics of interest in network engineering. I submit, therefore, that if something is not resilient now, but becomes so later on, there must be a process (or series of interrelated processes) that occurs as a business, in part or as a whole, moves from being exposed to disruption of critical resources toward being uninterruptible.

### The Infrastructure and Superstructure of Resilience

There is a difference between a business that has resilient resources and a business that is resilient. True enough, "uninterruptibility" (if there is such a word) must be based on a resilient infrastructure, including people, processes, facilities and technology. A number of strategies present themselves to achieve these ends: geographic dispersion, resource redundancy, outsourcing (and contingent outsourcing), duplication and path diversity, to name a few. Accepting that any resource is vulnerable to disruption and destruction in a worst-case scenario, the underlying assumption of resilience is that an organization must have more than one of any critical resource and that those must be far enough apart that the same event cannot make both simultaneously unavailable. Such solutions are expensive and introduce the possibility of causing more problems (e.g., latency, conflicting directions, integrity flaws, sluggish performance) than the cure is worth.

Thus, organizations should move toward resilience with careful determination to ensure that prudence and cost-effectiveness are observed. If unstopplable resources are the infrastructure, they need to fit under a superstructure of management and organizational control that oversees the transformation to resilience.

### Business Continuity Management

One might think that the business continuity management (BCM) function would be the most important part of that superstructure. However, BCM deals with keeping an organization functioning after a period of downtime. The

objective of resilience is to not experience downtime at all or, at least, not have it interrupt the business.<sup>3</sup> Many BCM functions are in the vanguard within their organizations in building resilience. Sadly, many such functions that I have seen are either just beginning recovery plans or are involved in nothing more than maintaining them. Disruptions are the *raison d'être* of business continuity; without them, there would be nothing for the BCM function to do. And, indeed, resilience is meaningful only if it is embedded in the quotidian operations of an organization, without the oversight of BCM.

That is not to say that the function does not have a role to play in resilience. Its talents and perspectives around assessment and analysis are valuable to determine the variable need for resilience in operations and management. Not everything needs to be uninterruptible. Absolutes should be avoided; there may be some brief stoppage but its effects would need to be negligible to achieve resilience. Planning and testing are less meaningful when there are no outages to be planned for and no tests of those outages to conduct. Organizations are resilient when resilience is business as usual (BAU).

### Governance and Risk Management

BAU does not imply the absence of management. Businesses are not music boxes that spin on their own and only need someone to wind the spring occasionally. Governance and oversight are especially important for resilient organizations. If the mechanisms that keep the business going do fail, then the skills of recoverability may have atrophied. In the transformation to resilience there is a subtle line that may be crossed, in which confidence in uninterruptibility supplants the vigilance for recovery. This must be a well-managed process to find a balance, a middle path, between complacency and being overly cautious.

This balance may be thought of as risk management, in that the risk of downtime must be addressed with equal concern for expense, complexity and inefficiency. There is a risk of putting all of one's eggs in a single basket, but there is also a limit on the number of baskets in which to put them. There is definitely a cost-benefit calculation to be made, but equally, there is a risk-benefit calculation. For example, having only one data center is manifestly risky. To avoid all data loss, at least given current technology, two data centers need to be relatively close to one another, close enough that they might both be susceptible to a regional event, such as a hurricane or a toxic chemical spill. In that case, is three the right number, two close and one far? Why not four? Or 10? At what point does the virtue of resilience come up against the

sins of wastefulness and incompatibility? The transformation to resilience cannot be carried out without critical forethought and careful attention to risks and requirements.

## Compliance and Improvement

Certain industries have an explicit need for resilience due to the nature of their business and often because of the regulatory requirements they face. For example, the risks to the underlying stability of national economies have caused regulators in many countries to require resilience in certain aspects of the financial services industry. In the US, certain financial activities require banks to “maintain sufficient geographically dispersed resources, including staff, equipment and data”<sup>4</sup> to resume business rapidly in the event of a disruption. Similar guidance has been issued, from London to Singapore<sup>5</sup> and around the world.

To be compliant with regulations, which are usually codification of good practice, there need to be mechanisms to measure and report on the effectiveness of the transformation to resilience. If one accepts the balance of risk and benefit discussed previously then it follows that the balance can be upset by changing business, technical, legal and environmental realities. Without an objective way of determining if there is a need for more or less resilience in any given function at any given time, it is likely that an organization will, over time, either retain too much risk or spend too much money. It should come as no surprise to the readers of the *Journal* that auditing is essential to measurement and reporting. I also advocate a more active role in these processes for the BCM function, with its specialized insights. A resilient enterprise must be led by management that, in a phrase, “gets it.”

The very concept of transformation implies change over time. The purpose of measuring is to determine the direction and speed of the movement. Dr. Werner Heisenberg said that one cannot simultaneously know both speed and direction, so the best one can hope for is educated uncertainty. In my experience, the gap in time between the recognition of the need for resilience and its achievement means that the initial analyses are inaccurate by the time the solution is implemented. This is not entirely bad, so long as the overall trend is toward improvement in managing risk and cost. A lack of precision is endurable, perhaps even acceptable, as long as there is a sense that external change is reliably driving an organization toward risk reduction at an affordable price.

## Endnotes

- <sup>1</sup> “The Resilient Toothbrush,” *Information Systems Control Journal*, vol. 2, 2008
- <sup>2</sup> It is worthwhile to define terms here. “Resilient” is described by Merriam-Webster ([www.merriam-webster.com](http://www.merriam-webster.com)) as “capable of withstanding shock without permanent deformation or rupture” or “tending to recover from or adjust easily to misfortune or change.” For the purposes of this article, the simple word “uninterruptible” will do just fine.
- <sup>3</sup> See “Downtime and Data Loss,” *Information Systems Control Journal*, vol. 5, 2006.
- <sup>4</sup> Federal Reserve System, *et al*, “Interagency Paper on Sound Practices to Strengthen the Resilience of the U.S. Financial System,” USA, 2003
- <sup>5</sup> Financial Services Authority, Resilience Benchmarking Project, UK, 2005. The Monetary Authority of Singapore in its Guidelines on Business Continuity Planning (2003) has the same line of thought as this article, specifically, “[Banks] should take into account both aspects of resilience and recovery, as well as the nature, scale and complexity of their businesses.”

**Steven J. Ross, CISA, CBCP, CISSP**

is a director at Deloitte. He welcomes comments at [stross@deloitte.com](mailto:stross@deloitte.com).

The advertisement features a central white box with the text "The Next Generation GRC Solution". Surrounding this box are four colored squares, each containing a logo: "HighPoint Audits" (yellow), "HighPoint Assessments" (red), "HighPoint Controls" (purple), and "HighPoint Policies" (blue). Below the central box, the text "HighPoint Enterprise from Favored Solutions" is displayed, followed by a description: "A new breed of browser-based software addressing the management of Governance, Risk and Compliance". At the bottom, the "Favored Solutions" logo is shown with contact information: "1-832-261-4747" and "www.favoredsolutions.net". To the right, a list of features is provided: "Internal Audit Management", "Risk Assessments and Analytics", "Enterprise Risk Management", "Internal Controls Management", "IT Governance", "Policies and Procedures", "Workflow Powered", and "Executive Reporting and Dashboards". The bottom right corner features the "INDUSTRY LEADER" logo from "The Institute of Internal Auditors".



# IT AUDIT BASICS

## Beyond the IT in IT Audit

**Tommie W. Singleton, Ph.D.,  
CISA, CITP, CMA, CPA**

is an associate professor of information systems at the University of Alabama at Birmingham (USA), a Marshall IS Scholar and a director of the Forensic Accounting Program. Prior to obtaining his doctorate in accountancy from the University of Mississippi (USA) in 1995, Singleton was president of a small, value-added dealer of accounting information systems (IS) using microcomputers. In 1999, the Alabama Society of CPAs awarded Singleton the 1998-1999 Innovative User of Technology Award. Singleton is the ISACA academic advocate at the University of Alabama at Birmingham. His publications on fraud, information technology (IT)/IS, IT auditing and IT governance have appeared in numerous publications, including the *Information Systems Control Journal*.

One of the common characteristics of those coming into the IT audit profession is their interest, skills, abilities or knowledge about IT. There is a little “geek” in most of us. In performing IT audits, it is easy to get caught up in the IT part and lose sight of the nontechnical matters. The big picture includes many matters, some of which include the overriding business objective (not just those of the IT being reviewed), risk assessment and evaluation, and “soft” skills (i.e., communications, interpersonal). While these fundamental matters have received much press and discussion, they often do not work their way into the IT auditor’s behavior. The ability to function well in these areas is necessary for all IT auditors to fulfill their duties and obligations. This article attempts to illustrate to those new to the field, and maybe other IT auditors, some of the important issues beyond the IT in IT audit.

### The Business

Every business that needs the services of IT audit should have established organizational strategies. Those strategies begin at the business model, where the entity describes in some detail how it plans to generate revenues, obtain customers and deal with supply-chain-type issues regarding its goods or services. From that model, executive management develops goals, individual strategies and objectives to fulfill the business model. Those things should be written, and those documents and plans are critical to any audit. Anything that is assessed must be measured against some benchmark. While it is tempting to assess IT against what one knows about how IT could or should perform, that cannot be done in isolation from the way the business intends to operate. Indeed, an effective benchmark, standard of measure, should be developed in the context of the way the business operates and its intended goals and objectives. In fact, a basic and critical objective of IT audit is the integration of IT into the business processes, objectives and overall environment. Therefore, the

business model and its accoutrements are the context of the IT audit procedures, evidences and analyses.

One example would be determination of what specific IT control should be employed by the organization in a certain situation. To determine what controls should be operating, there must be some context, some benchmark. That context and benchmark should be determined using the business model and associated plans. That is, what control should be in place that would be effective in ensuring management’s ability to meet the organization’s goals, objectives and strategies and, eventually, see the business model come to fruition successfully? If IT auditors use that kind of thought process, they may come to a different conclusion than when using one based on what the auditors think should be in place when considering solely IT matters, not the “big picture.”

Another example would be remediation of an assessed control weakness in IT. When the IT auditor discusses remediation with management or reviews the remediation activities, what is the benchmark of an appropriate or successful remediation? How does one know the weakness is “better” or “fixed”? That is, the weakness must be measured against some prescriptive solution. The prescriptive solution should be determined by its impact on the organization’s ability to meet its goals and objectives associated with the business model, and not just on what a technologically savvy solution offers or some ideological idea of what it should be. The bottom line is, without businesses and organizations, there is no IT audit, and one must understand the context to effectively audit IT in that realm.

### Risk Assessment

While the business environment is the “sandbox” of IT audits, risk assessment is the “shovel,” the basic tool auditors use to shape audits. *Control Objectives for Information and related Technology* (COBIT®), the Committee of Sponsoring Organizations of the Treadway Commission (COSO) model,



the Public Company Accounting Oversight Board (PCAOB) standards, ISACA's IS Auditing Standards, the Institute of Internal Auditors guidelines, and every other credible source of audit regulation or professional guidance addresses risk assessment. It is hard to think of any type of audit that is not planned, performed or evaluated through a risk assessment. Still, it is easy to conduct an audit that lacks the rigorous, top-to-bottom and continuous approach to risk assessment. Moreover, modern IT elements and business assets are typically intangible and difficult to measure, so defining probability and impact is difficult at best and, at worst, barely feasible. When the IT auditor is planning the audit, what is the method for deciding the "best" set of tests and individual procedures? How does one reasonably reach conclusions based on the results?

As stated previously, the audit should be designed with the "big picture" in mind. Risk assessment should be viewed similar to a funnel system, with high-level risks spiraling, effecting downward causation on lower-level risks to specific objectives. During the course of the audit, risk assessment should be a process and a mindset, not an initial isolated step, document or meeting. When feedback is continually fed back into the initial assessment in performing procedures and evaluating results, true risks are likely to be mitigated. While few risks can be tangibly and definitely measured, they can be better understood with this balance of holistic and analytical viewpoints, and a continual focus on the implications of audit objectives.

For those without experience in auditing, the judgment needed to evaluate risk is difficult to explain. Expertise in judgment certainly requires experience, but any progress in the matter requires a mindset aware of, and sensitive to, risk dynamics. Experienced auditors should ensure younger auditors absorb the threats and implications associated with the overall, and specific, audit procedures. For those new to the field of IT audit, one of the best questions to ask is: "what exactly is the risk?" Even better would be to evaluate the situation and say to a senior auditor: "I believe the risk probability is X and the impact would be Y. What do you think?" Additionally, the risk process must be documented to establish why and how procedures were performed, and why the results naturally follow.

What are the risks identified by management in regard to reaching their goals and objectives, in working out the business model successfully? What are the obvious risks of material misstatement or other audit objectives? Then, the IT auditor should examine areas of significant risk (e.g., "high" residual risk) and determine tests and procedures. The best test for risk X would then be designed based on the context of the entity's goals and objectives, and how risk relates to them.

One way for any IT auditor to improve risk assessment is to leverage management's intimate knowledge. While reliance on management's knowledge is a difficult balance, management should know as well as anyone what the risks are, and auditors should not ignore this fact. For instance, the IT auditor is onsite for a few days, or at most a few weeks,

each year. Management is there year-round and, as a result, should have in-depth knowledge of the business, including its risks. Using management's unique perspective on risks can expand and clarify the understanding of the overall environment and the specific considerations necessary to evaluate any given audit objective.

## Soft Skills

Soft skills (defined here as communication and interpersonal skills) are often the critical success factor in an IT audit. This aspect of IT audit is overlooked frequently, but every IT audit (and in fact every business purpose) involves communication to another party. Therefore, verbal and written communication skills, and the ability to establish and maintain positive relationships, are vital to achieving effectiveness in an IT audit. For years, professionals have derided the level of communication skills among university

accounting graduates. Even in university programs where these skills are taught, students often tend to not take writing and speaking skills seriously.<sup>1</sup> In the workplace, soft skills can determine the difference between success and failure,

regardless of the technical results. It is not uncommon for someone to have enough charisma to be successful despite major weaknesses in other areas.

The fact is, soft skills are essential to being an effective IT auditor, and even more essential to a successful career in IT audit. The bottom line of any IT audit is communicating results. The delivery of the results of the IT audit necessitates the use of either written or oral communication. Sometimes, the IT auditor is telling management that the controls are "material weaknesses" or is giving some other bad news. The above circumstance of asking for management to assist in providing insights into the development of tests and procedures is another example of the need for soft skills (interpersonal skills, in this case).

Every document and every conversation should have an effective thesis (i.e., what is the point?). All of the content should be focused on that thesis, which in IT audit is inevitably centered upon the relevant risk(s). For example, the IT auditor may write up a control weakness by providing logical, well-documented reasons for management to remediate an identified risk exposure. Longer documents should employ the use of topic sentences, which should be the first sentence in a paragraph. The ideas themselves should be organized in the document in a cogent manner; they should naturally flow from one idea to the next, coherently supporting the thesis. These two aspects are critical to effective writing. One tip is to keep the communication matter simple; if there are more than three major points, the author (IT auditor) may have trouble communicating effectively with the audience.

In written communications, good grammar, correct spelling and other basic writing rules should be observed. Another factor is the level and structure of the writing. It should be addressed to the audience in terms of tone, overall level of readability,<sup>2</sup> and choice of terms (e.g., acronyms).<sup>3</sup> Eliminating

---

*In the workplace, soft skills can  
determine the difference between  
success and failure.*

---

unnecessary words is one way to improve communications; for example, instead of using “in order to,” use “to.” Where appropriate, use bullet points or outlines to condense and customize material to fit the audience, particularly for higher levels of management.

Interpersonal skills, such as nonverbal communication and understanding personality styles, are also important for IT auditors. Nonverbal communication suggests an individual’s level of attentiveness and responsiveness. Paying attention to the audience’s posture, expressions and mannerisms can reveal this fact. More broadly, understanding personality styles, such as differences between relationship-driven and task-driven styles, can enhance the IT auditor’s communication effectiveness. The key is to be aware of your own and your audience’s general tendencies and expressions at the moment.

## Conclusion

IT audits necessarily have a focus on IT skills, knowledge and issues, but there is a bigger picture beyond the IT aspect of IT audit. Some of the more important big-picture issues are using the business model, and its associated plans and objectives, as the context for the IT audit; remembering to place decisions in the venue of risk assessment; and employing soft skills effectively.

## Endnotes

- <sup>1</sup> As a university professor of an IT audit course, I am constantly distressed by the overall writing skills of accounting majors.
- <sup>2</sup> One rule of thumb is to write at a level of education well below that expected of the audience, so it will be easy to read and follow the language and content.
- <sup>3</sup> One highly recommended resource is the May, Claire B.; Gordon S. May; *Effective Writing: Handbook for Accountants*, 7<sup>th</sup> Edition, Prentice Hall, 2005.

## Author’s Note:

A special thanks to Aaron Singleton, CPA, CISA, auditor in systems and process assurance for PricewaterhouseCoopers in Raleigh, North Carolina, USA, for his contributions to this article.

SERVING IT GOVERNANCE PROFESSIONALS



**Certification—Your Passport to Success**  
**[www.isaca.org/certification](http://www.isaca.org/certification)**

# IT Governance Global Status Report 2008:

## An Excerpt

By Dirk Steuperaert, CISA

**I**nsufficient IT staff availability, service delivery issues and difficulty proving the value of information technology continue to concern executives at organisations around the world, according to a new report by the IT Governance Institute (ITGI).

ITGI recently commissioned a global survey of 749 CEO-/CIO-level executives in 23 countries to determine executives' IT governance priorities and the IT-related problems their organisations have faced. According to IT Governance Global Status Report—2008, which is available as a complimentary download at [www.itgi.org](http://www.itgi.org), 58 percent of respondents noted an insufficient number of staff, compared to 35 percent in 2005. Also, 48 percent said that IT service delivery problems remain the second most common problem, and 38 percent point to problems relating to staff with inadequate skills. Thirty percent of respondents also reported problems anticipating the return on investment (ROI) for IT expenditures.

The study is a follow-up to ITGI's 2003 and 2005 surveys and tracks IT governance trends over the past four years. The following is the executive summary from the 2008 publication. Readers are encouraged to visit [www.itgi.org](http://www.itgi.org) to download the full document.

### Executive Summary

In 2007, PricewaterhouseCoopers (PwC) was commissioned by the IT Governance Institute (ITGI) to conduct the third global survey on IT governance, resulting in this *IT Governance Global Status Report—2008*.

The IT governance survey was conducted from July 2007 to October 2007 and focuses on specific topics such as IT risks and value delivery.

### Project Objectives

The purpose of the research was to reach members of the C-suite to determine their sense of priority and actions taken relative to IT governance, as well as their need for tools and services to help ensure effective IT governance.

This high-level objective was translated into the following more detailed objectives:

1. Survey and analyse the degree to which the concept of IT governance is recognised, established and accepted within boardrooms and especially by chief information officers (CIOs).
2. Determine what level of IT governance expertise exists and which frameworks are known and are (or will be) adopted.

3. Measure the extent to which ITGI's own framework, *Control Objectives for Information and related Technology* (COBIT), is selected and how it is perceived.

### Survey Sample

Researchers contacted CIOs and chief executive officers (CEOs). The total number of interviews conducted was 749, of which 652 were from a random sample of organisations; 71 were known as COBIT users and 26 were experienced COBIT users.

### Global Reach

The interviews were conducted worldwide (in 23 countries), and all continents/regions were represented.

### Historical Data

Because this report is the third consecutive undertaking of this IT governance research project, the project team was able to use historical data from the 2004 and 2006 research reports (based on 2003 and 2005 surveys) to discover trends in a number of areas.

### How to Read The Report

The report contains six chapters:

- Chapter 1 explains the methodology used to conduct the survey.
- Chapter 2 highlights the survey results in 13 key messages.
- Chapter 3 focuses on the detailed survey results supporting the 13 key messages.
- Chapter 4 presents trends and issues in IT risk management.
- Chapter 5 identifies trends and issues in IT value management.
- Chapter 6 contains the results of the funnel analysis.
- The appendix includes the questionnaire and further information on the compound problem index.
- There is a table of figures at the end of the report.

### Key Findings of the Survey

The 13 key messages that have been identified during the analysis of the survey reflect important findings from the results of the survey:

1. Although championship for IT governance within the enterprise comes from the C-level, in daily practice IT governance is still very much a CIO/IT director issue. The few non-IT people in the sample have a much more positive view of IT than do the IT professionals themselves.



2. The importance of IT continues to increase.
3. Self-assessment regarding IT governance has increased and is quite positive.
4. Communication between IT and users is improving, but slowly.
5. There is still substantial room for improvement in alignment between IT governance and corporate governance—as well as for IT strategy and business strategy.
6. IT-related problems persist. While security/compliance is an issue, people are the most critical problem.
7. Good IT governance practices are known and applied, but not universally.
8. Organisations know who can help them implement IT governance, but appreciation for the available expertise and delivery capability is only average.
9. Action is being taken or plans are underway to implement IT governance activities. A large increase is evident when compared to the 2006 report.
10. Organisations use the well-known frameworks and solutions.
11. COBIT awareness has exceeded 50 percent, and adoption and use remain around 30 percent.

- a. Twenty-five to 35 percent of respondents apply COBIT to the letter or are very strict.
  - b. Fifty percent of respondents indicate that COBIT is 'one of the reference sources'.
  - c. In general, there is high appreciation of COBIT, as has been seen in prior reports.
12. More than half of the respondents apply or plan to apply Val IT principles, but are not familiar with the Val IT brand itself.
  13. Major obstacles to adoption and use of Val IT principles include uncertainty regarding the return on investment (ROI) and lack of knowledge/expertise.

#### **Dirk Steuperaert, CISA**

is an independent IT governance consultant through his new firm IT-In-Balance. Until March 2008, he was a director within PricewaterhouseCoopers Belgium, where he was responsible for IT governance advisory services. The bi-yearly IT governance survey is commissioned to PricewaterhouseCoopers by ITGI, and Steuperaert is the project leader for the survey. He is also a member of the COBIT Steering Committee, assisting in the further development of COBIT.

iate audit scope, lead and coach the  
aff to produce a work product within  
he ideal candidate will be technically  
ave a strong IT Audit background.  
ly desired.

#### **Supervisor Island**

will function as an Auditor in Charge  
ite audit scope, lead and coach support  
is noted during the audit engagement  
efficiency, IT Audit experience, CISA,  
strong leadership skills and team spirit

tional benefits. Interested candidates,  
**employment.**

: is an equal opportunity/  
committed to building  
ce. M/F/D/V.

## **ExamMatrix Smarter, Faster**



## **CISA Exam Review**

Authored by SRV's S. Rao Vallabhaneni

- 1,700 Multiple Choice Questions
- Personalized Study Sessions
- Pass or Refund Guarantee

www.ExamMatrix.com/ISJ  
www.ExamMatrix.com  
1.800.272.PASS

**EXAMMATRIX**™



# Network Traffic Control

*High Capacity, Safe, Secure; It's Hardware.*

Capable of supporting more than 4,000 network users, SwitchMaster® assures a controlled access environment using rugged and precise mechanical and optical movements that deliver the unequalled reliability of hardware.

System administration is simplified for fast and easy monitoring of individual users with automatic shut-off control when tampering is detected. Only the System Administrator can restore the connection, moving stress from the administrator directly to the prospective intruder.

SwitchMaster ganged A-B Switches with **Plug 'n' Protect™** design keep you transactional with real-time asset protection. You can add advanced Category 6 performance that supports the 10 gigabit/sec information transfer rates of 802.3an 10GBase-T.

**SwitchMaster – another information padlock from the designers of the Government-Validated SecureSwitch® family of products.**  
Market Central® | 500 Business Center Drive, Pittsburgh, PA 15205

© 2008 Market Central, Inc.



## SwitchMaster®

*is the **superior choice** for network access control and backup switches – providing ultra-reliable, hardware-driven security.*

**Confidently regulate the flow of a multi-user network with the SwitchMaster solution.**

**Call our design engineers today, or visit our web site.**

412 494 2800 | [www.secureswitch.com](http://www.secureswitch.com)  
[info@secureswitch.com](mailto:info@secureswitch.com)

## ISACA Member and Certification Holder Compliance

The specialised nature of IS auditing and the skills necessary to perform such audits require standards that apply specifically to IS auditing. One of the goals of ISACA is to advance globally applicable standards to meet its vision. The development and dissemination of the IS Auditing Standards are cornerstones of ISACA's professional contribution to the audit community. The framework for the IS Auditing Standards provides multiple levels of guidance:

■ **Standards** define mandatory requirements for IS auditing and reporting. They inform:

- IS auditors 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 IS Auditing Standards. The IS auditor 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 IS Auditing Guidelines is to provide further information on how to comply with the IS Auditing Standards.

■ **Procedures** provide examples of procedures an IS auditor might follow in an audit engagement. The procedure documents provide information on how to meet the standards when performing IS auditing work, but do not set requirements. The objective of the IS Auditing Procedures is to provide further information on how to comply with the IS Auditing Standards.

**Control Objectives for Information and related Technology (CobiT)** is an IT governance framework and supporting tool set that allow 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 organisations. It emphasises regulatory compliance, helps organisations 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 IS auditors; therefore, its usage enables the understanding of business objectives and the 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). As defined in the CobiT framework, each of the following related products/elements is organised by IT management process:

■ **Control objectives**—Generic statements of minimum good control in relation to IT processes

■ **Management guidelines**—Guidance on how to assess and improve IT process performance, using maturity models; Responsible, Accountable, Consulted and/or Informed (RACI) charts; goals; and metrics. They provide a management-oriented framework for continuous and proactive control self-assessment specifically focused on:

- Performance measurement
- IT control profiling
- Awareness
- Benchmarking

■ **CobiT Control Practices**—Risk and value statements and 'how to implement' guidance for the control objectives

■ **IT Assurance Guide**—Guidance for each control area on how to obtain an understanding, evaluate each control, assess compliance and substantiate the risk of controls not being met

The titles of issued documents follow.

### IS Auditing Standards

- S1 Audit Charter Effective 1 January 2005
- S2 Independence Effective 1 January 2005
- S3 Professional Ethics and Standards Effective 1 January 2005
- S4 Professional Competence Effective 1 January 2005
- S5 Planning Effective 1 January 2005
- S6 Performance of Audit Work Effective 1 January 2005
- S7 Reporting Effective 1 January 2005
- S8 Follow-up Activities Effective 1 January 2005
- S9 Irregularities and Illegal Acts Effective 1 September 2005
- S10 IT Governance Effective 1 September 2005
- S11 Use of Risk Assessment in Audit Planning Effective 1 November 2005
- S12 Audit Materiality Effective 1 July 2006
- S13 Using the Work of Other Experts Effective 1 July 2006
- S14 Audit Evidence Effective 1 July 2006
- S15 IT Controls Effective 1 February 2008
- S16 E-commerce Effective 1 February 2008

### IS Auditing Guidelines

- G1 Using the Work of Other Auditors and Experts Effective 1 March 2008
- G2 Audit Evidence Requirement Effective 1 May 2008
- G3 Use of Computer-assisted Audit Techniques (CAATs) Effective 1 March 2008
- G4 Outsourcing of IS Activities to Other Organisations Effective 1 May 2008
- G5 Audit Charter Effective 1 February 2008
- G6 Materiality Concepts for Auditing Information Systems Effective 1 May 2008
- G7 Due Professional Care Effective 1 March 2008
- G8 Audit Documentation Effective 1 March 2008
- G9 Audit Considerations for Irregularities Effective 1 March 2000
- G10 Audit Sampling Effective 1 March 2000
- G11 Effect of Pervasive IS Controls Effective 1 March 2000
- G12 Organisational Relationship and Independence Effective 1 September 2000
- G13 Use of Risk Assessment in Audit Planning Effective 1 September 2000
- G14 Application Systems Review Effective 1 November 2001
- G15 Planning Revised Effective 1 March 2002
- G16 Effect of Third Parties on an Organisation's IT Controls Effective 1 March 2002
- G17 Effect of Non-audit Role on the IS Auditor's Independence Effective 1 July 2002
- G18 IT Governance Effective 1 July 2002
- G19 Irregularities and Illegal Acts Effective 1 July 2002
- G20 Reporting Effective 1 January 2003
- G21 Enterprise Resource Planning (ERP) Systems Review Effective 1 August 2003
- G22 Business-to-consumer (B2C) E-commerce Reviews Effective 1 August 2003
- G23 System Development Life Cycle (SDLC) Reviews Effective 1 August 2003
- G24 Internet Banking Effective 1 August 2003
- G25 Review of Virtual Private Networks Effective 1 July 2004
- G26 Business Process Reengineering (BPR) Project Reviews Effective 1 July 2004
- G27 Mobile Computing Effective 1 September 2004
- G28 Computer Forensics Effective 1 September 2004
- G29 Post-implementation Review Effective 1 January 2005
- G30 Competence Effective 1 June 2005
- G31 Privacy Effective 1 June 2005
- G32 Business Continuity Plan (BCP) Review From IT Perspective Effective 1 September 2005
- G33 General Considerations for the Use of the Internet Effective 1 March 2006
- G34 Responsibility, Authority and Accountability Effective 1 March 2006
- G35 Follow-up Activities Effective 1 March 2006
- G36 Biometric Controls Effective 1 February 2007
- G37 Configuration and Release Management Effective 1 November 2007
- G38 Access Controls Effective 1 February 2008
- G39 IT Organisation Effective 1 May 2008

### IS Auditing Procedures

- P1 IS Risk Assessment Measurement Effective 1 July 2002
- P2 Digital Signatures and Key Management Effective 1 July 2002
- P3 Intrusion Detection Systems (IDS) Review Effective 1 August 2003
- P4 Malicious Logic Effective 1 August 2003
- P5 Control Risk Self-assessment Effective 1 August 2003
- P6 Firewalls Effective 1 August 2003
- P7 Irregularities and Illegal Acts Effective 1 December 2003
- P8 Security Assessment—Penetration Testing and Vulnerability Analysis Effective 1 September 2004
- P9 Evaluation of Management Controls Over Encryption Methodologies Effective 1 January 2005
- P10 Business Application Change Control Effective 1 October 2006
- P11 Electronic Funds Transfer (EFT) Effective 1 May 2007

**Standards for Information System Control Professionals** Effective 1 September 1999

#### 510 Statement of Scope

- .010 Responsibility, Authority and Accountability

#### 520 Independence

- .010 Professional Independence
- .020 Organisational Relationship

#### 530 Professional Ethics and Standards

- .010 Code of Professional Ethics
- .020 Due Professional Care

#### 540 Competence

- .010 Skills and Knowledge
- .020 Continuing Professional Education

#### 550 Planning

- .010 Control Planning

#### 560 Performance of Work

- .010 Supervision
- .020 Evidence
- .030 Effectiveness

#### 570 Reporting

- .010 Periodic Reporting

#### 580 Follow-up Activities

- .010 Follow-up

**Code of Professional Ethics** Revised May 2003

### ISACA 2007-2008 Standards Board

- Chair, Ravi Muthukrishnan, CISA, CISM, FCA, ISCA, Capco IT Services India Pte. Ltd., India
- Brad David Chin, CISA, CPA, Google Inc., USA
- Sergio Fleginsky, CISA, AKZO Nobel, Uruguay
- Maria Gonzalez, CISA, CISM, Department of Defence, Spain
- John Ho Chi, CISA, CISM, CBCP, CFE, Ernst & Young, Singapore
- Andrew J. MacLeod, CISA, CIA, FCPA, MACS, PCP, Brisbane City Council, Australia
- John G. Ott, CISA, CPA, AmerisourceBergen, USA
- Jason Thompson, CISA, CIA, KPMG, USA
- Meera Venkatesh, CISA, CISM, ACS, CISSP, CWA, Microsoft Corp., USA



# IT VALUE

## Recognising the Need for Val IT: Identifying Tipping Points for Value Management

By Sarah Harries and Peter Harrison, FCPA

This is the first of six articles to be published in this column on the practicalities of introducing and establishing Val IT™. These articles draw from the authors' many years of experience working with enterprises to introduce value management.

The remainder of the series will cover:

- The Five Starting Steps to Introduce Val IT
- Practical Guidance on Establishing Value Governance
- The Challenges of Implementing Portfolio Management
- Benefits Realisation and Programme Management—Beyond the Business Case
- Critical Success Factors for Introducing Val IT

Executives, even if they are aware of the need for more effective governance and management of information technology (IT), may not recognise that many of the day-to-day business challenges they face involve issues of value management. Val IT provides proven value management principles, processes and practices to enable enterprises to maximise the delivery of business value from investments involving IT.

This article identifies some of the most common tipping points—the pain points or “trigger” events that are likely to, or at least should, spur executives to improve their enterprise's value management practices.

Experience shows that the tipping points can come from two sources:

- **Internal events**—Experiences that bring into question the contribution of IT to the enterprise. Examples include major IT project failures, serious budget overruns, the enterprise's inability to absorb the changes delivered by new technologies, business executives not understanding the business value of IT, and IT executives (or indeed major IT suppliers) needing to prove the value to the business of the services delivered.
- **External events**—Influences from beyond the enterprise that necessitate the changing of IT priorities. Examples include mergers and acquisitions, a major shift in the marketplace with respect to competitors' actions or

economic conditions and the need to share services or outsource a business process.

### Internal Tipping Points

The most common internal tipping points include:

- **A major IT project failure**—Every enterprise has had at least one of these. Enterprise resource planning (ERP) and customer relationship management (CRM) investments are classic examples. A major IT project has become a disaster when/if it is exhibiting all or a combination of the following symptoms:
  - Being delivered too late
  - Cost overruns
  - Not delivering the benefits

Such a project probably struggles on until it is either declared closed with nothing much delivered, or a new chief executive officer (CEO) kills it. Sometimes it gets

relaunched with a new name only to suffer the same fate. Such failures, apart from being costly, can be highly visible, resulting in bad press, reduced market valuation and/or damage to the enterprise's credibility. Executives ask:

- Where is the value expected from this IT project?
- How could this go so terribly wrong? Why didn't anyone warn us?
- We have trained our people in project management, how could this project fail?
- Was this our fault or the supplier's fault?

This is a fairly common tipping point. No one likes costly failures, especially highly visible ones, and executives who have experienced major investment failures do not want to get burnt again.

- **Recognition by executives that they do not know everything they should about their IT-related expenditures**—This is especially likely with the appointment of a new CEO, chief financial officer (CFO), chief information officer (CIO) or IT director. Questions may be asked by the executive that probe the completeness

---

*Val IT provides proven value  
management principles.*

---

and effectiveness of their governance processes. These questions may include:

- Do we have an inventory of assets and projects/investments?
- Are we investing in projects that align to what the business currently wants to do?
- How do we prioritise the allocation of scarce resources to deliver maximum business value and how do we define ‘business value’ anyway?
- Do we have ownership and accountability for the business change and outcomes we expect from our IT projects?
- Why are we continuously juggling investments and changing priorities within our limited capabilities and constraints?

The tipping point comes when unsatisfactory answers create anxiety at the executive level as to whether business value from the IT spend is being maximised—or realised at all.

- **Business executives not seeing proof of the business value delivered by IT**—IT is a key enabler for the business to operate and grow successfully and to create value. However, the contribution of IT to the success of the enterprise is frequently implicitly assumed by proponents of technology rather than explicitly stated and, therefore, is difficult to justify and even harder to measure. In this environment, how can executives feel comfortable with business benefits that are promised from new investments involving IT, and how can they determine if they were realised? The tipping point comes when executives are asked to approve investment decisions in cases where they can see no readily identified business justification to do so.

## External Tipping Points

The external tipping points include:

- **Major shift in the enterprise’s situation in relationship to the market, economy, competitors, etc.**—Market and economic factors may necessitate the enterprise to quickly respond or suffer the consequences. Executives will be asking:
  - How fast can we introduce new products (with associated enabling of IT)?
  - How could we handle a merger/acquisition in terms of integration of IT?

The tipping point comes when the executives see that the speed of decision making and responsiveness of the enterprise to rearrange priorities in response to market and economic changes is ineffective and keeping the enterprise lagging behind its competitors.

- **Regulatory changes or budget cuts**—Enterprises, particularly heavily regulated ones or those in the public sector, face the need to respond in a timely fashion to

legislative, policy and funding changes. Executives will be asking:

- Can we comply with new regulatory requirements without impacting our transformational change programmes?
- How do we best manage the impact to our current projects of a budget-funding cut?

The tipping point comes when the executives realise they cannot readily provide the answers to the ‘what ifs’ and analyse the impact of externally mandated changes.

## The Tipping Point Challenge

How many of these tipping points can you recognise within your own enterprise? It is not enough to recognise them as problems—the challenge for business and IT executives is to take action. The Val IT framework provides useful guidance on proven processes and practices that enable effective governance of investments involving IT. This guidance is found in the three domains of Val IT:

- **Value Governance (VG)**—Ensuring that value management practices are embedded in the enterprise
- **Portfolio Management (PM)**—Ensuring that the enterprise secures optimal value across its portfolio of investments involving IT
- **Investment Management (IM)**—Ensuring that the enterprise’s individual investments each contribute the value expected of them

### Sarah Harries

was with Fujitsu Services (UK) until 2008, specialising in value management (VM). She also chaired Fujitsu’s global VM community of interest. She is now benefits realisation manager at Openreach, a BT Group business.

### Peter Harrison, FCPA

is a principal and member of the value governance leadership team within Fujitsu Consulting Australia and New Zealand, and is a member of the Val IT Steering Committee.

## Editor’s Note:

The three initial publications of the Val IT project can be downloaded free from the ITGI web site, [www.itgi.org](http://www.itgi.org), and include: *Enterprise Value: Governance of IT Investments*, *The Val IT Framework 2.0*; *Enterprise Value: Governance of IT Investments, The Business Case*; and *Enterprise Value: Governance of IT Investments, The ING Case Study*. Readers are encouraged to review Val IT and share it with key governance stakeholders within their enterprises. Please visit [www.isaca.org/valit](http://www.isaca.org/valit) or contact Brian Selby at [bselby@isaca.org](mailto:bselby@isaca.org) for further information regarding Val IT.



# Five Questions With...

Luis Eduardo Toro Lobos, CISM

*Luis Eduardo Toro Lobos is national managing partner of consulting and enterprise risk services (ERS) at Deloitte Mexico. He manages more than 1,000 professionals and 35 partners in nine cities, and is regional managing partner of consulting in Latin America and the Caribbean.*

*His principal areas of expertise include internal audit and consulting, primarily in the financial, mining, retail and*

*government sectors. He has more than 25 years of experience establishing and maintaining frameworks to provide assurance. Those information security strategies are aligned with business objectives and consistent with applicable laws and regulations.*

*Away from the office he enjoys playing soccer, tennis and reading books from his favorite authors, Jim Collins and Michael Porter.*

## Question

**You have experience in IT audit and risk management. How do you see these two areas working together into the future?**

## Answer

During the past decade, control models have been a dominant factor in improving IT audit performance and managing organizational risk. Now, risk-based auditing pushes those models a step farther and points auditors toward the future.

Auditors have been trained to make detailed examinations of IT control systems, recommend cost-effective actions for improving IT control, and focus their audit planning, testing and reporting on IT controls in the business process.

Control models such as the IT Governance Institute® (ITGI™)'s *Control Objectives for Information and related Technology* (COBIT), Committee of Sponsoring Organizations of the Treadway Commission (COSO)'s frameworks, the IT Infrastructure Library (ITIL), and the International Organization for Standardization (ISO)'s ISO 27001 have been huge milestones in the progress of auditing and governance. Adoption of such models throughout the world has marked the first time ever that stakeholders worldwide have come to agree on a definition of internal and IT control. As a result, the major governance professions have reached a common understanding and made integration possible.

These models now need to be extended, however, so that IT auditors can use them differently and take the next step in risk management. Risk-based auditing (RBA) can address some of the important questions that controls-based auditing leaves unanswered. RBA is a major step toward improved IT audit performance and organizational risk management. IT auditors who have made the change to RBA have found increased management acceptance and greater integration of IT audit with other governance elements of risk management.

## Question

**What are some of the challenges you see facing IT departments in the near future?**

## Answer

Challenges to corporate networks are coming from a growing list of sources. These include increasing online instances where businesses are facing significantly increased threats to their networks, concurrently with high demand to provide additional capabilities. Since corporate networks are becoming more complex, with an increasing number of vulnerability points, including wireless access and virtual private networks (VPNs), there is an increasing threat to networks. Increasing threats and vulnerabilities to systems means that IT departments must acquire more sophisticated protection. With the advent of content-based attacks in e-mail and the Internet, where malicious code is spread across many packet payloads, implementation of managed security service provider (MSSP) capabilities is a must. Another emerging area of concern is the need for regulatory compliance and managing new government initiatives. Diverse organizations operating in multiple business disciplines of all types and sizes are facing regulatory requirements that did not exist only a few years ago. Finally, cost, complexity and expertise are required to effectively implement security. Often, deploying IT resources in-house to properly implement and manage a sophisticated network security solution is a significant challenge. The evolving nature of threats and growth in network size and complexity could lead to continuing and significant capital equipment expenditures.

## Question

**What enterprise risk management (ERM) trends are you seeing that will impact business in the near term?**

## Answer

As the result of the increasing costs of risk and compliance activities, enterprises are beginning to integrate compliance and risk management into a comprehensive ERM function and, thus, proactively address all sorts of risk, including operational



risk and the risk of noncompliance. In the last few years, many organizations have been challenged by a surge of new cross-industry and industry-specific regulations. Examples are the ubiquitous Sarbanes-Oxley Act, the US Patriot Act and, in the financial industry, the Basel II Accord. In many enterprises, regulations such as these have resulted in a multitude of individual compliance projects that consume a large share of available resources, thereby leading to significant costs. To attain and demonstrate compliance, enterprises have been gathering large amounts of historic financial and business data.

Similar to financial statement reporting and performance management, however, initial compliance management initiatives have been conducted with a rather backward-looking perspective, with penalty avoidance as the main goal. With their strong focus on periodic audits, expensive point projects geared to individual regulations have often failed to deliver additional value to the company. In fact, companies that have delegated regulatory compliance to the various lines of business often find that they have incurred costly duplication of effort. Due to the mounting expense and inefficiencies of compliance projects, businesses have started to embrace a new approach by treating noncompliance as a risk and, thus, embedding compliance management as part of a larger ERM approach geared to bringing greater transparency and value to the business. This resulted from the realization of the great potential that lies in the large amount of gathered compliance data. But, simply gathering data does not automatically provide business insights. Enterprisewide information needs to be integrated by focusing on data standardization and harmonization and through enterprisewide data governance. This integration of reporting disciplines and overall risk management principles at the corporate level helps the business change from simple compliance to increased business efficiency. Value for the company is created through the generation of information aimed at delivering insight into performance, growth and risk. This is paralleled by the mitigation of structural complexity through process and policy simplification, standardization and optimization.

### Question

**What are your thoughts around certifications and do you feel that they can advance or enhance someone's career? What certifications do you look for when hiring new members of your team?**

### Answer

Life-long learning is the rule today, rather than the exception, for IT professionals. Even in an IT sector wracked by skills shortages, it is the individuals who continually build on strong educational foundations, regularly adding new skills and expertise, who get the best jobs and promotions.

Having the qualifications (alone) will not get you the job; companies want appropriate soft skills and a good cultural fit as well. Oftentimes candidates are severely lacking in the soft skills like communication, meeting skills and assertiveness.

They may have a degree, but they are not useful to business until they learn how to work.

Young graduates are far more employable if they can gain some sort of work experience, either by working part time while at university or taking a first job as a co-op or intern where skills shortages are even more acute and they can learn some soft skills on the job. But even with this early experience, most young graduates still need to supplement their degree with certification.

The certification push is also prompting a subtle change in the marketplace; where once a good product succeeded on its own merits, today the success of products is increasingly about access to skills regarding that product. The more product-certified candidates in the market, the more likely that product will succeed.

What certification does not generally address is the development of so-called soft skills and, as noted earlier, they are critical for career advancement. Development and acceleration of individuals do not come from technical skills,

but from their ability to solve problems in teams; work on cross-cultural teams; present to small, medium and large groups; articulate ideas verbally and in written papers; and generally come across well. This is typically not taught at

universities, so it is left to the employer and the individual.

The types of certifications that we normally look for are consultants certified in product-specific tools, IT audit and security, and project management. Knowing someone has at least studied the concepts and has taken the steps to obtain the certifications gives that person a step up over someone who has not.

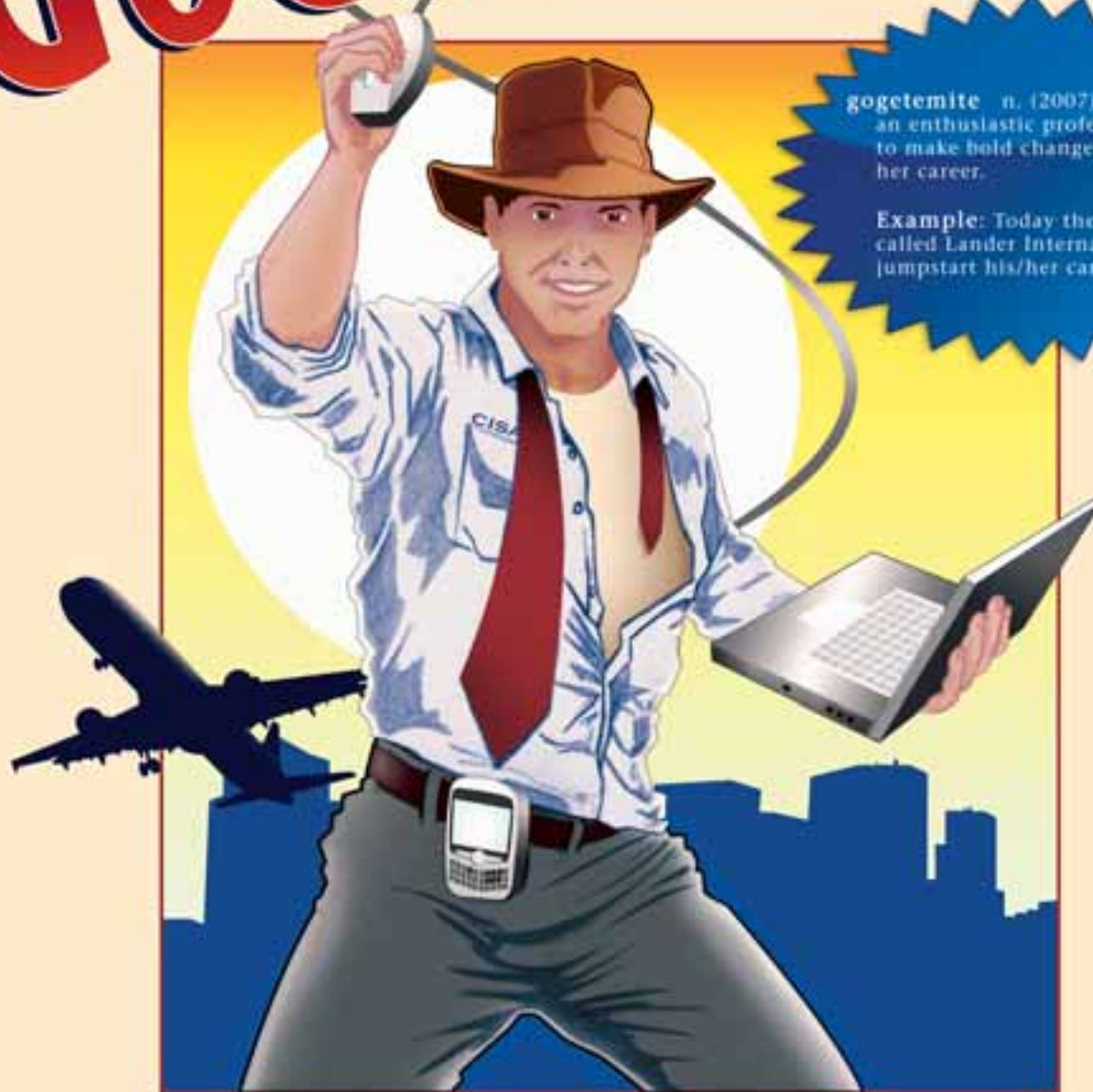
### Question

**What do you feel are a company's biggest workplace challenges and what are needed to improve them?**

### Answer

As companies sustain constant change, their ability to compete globally is being strained. Today's evolving workplace is the result of many factors: global competitiveness, mergers and acquisitions, and changing management and organizational structures. This dramatic transformation is affecting not only leaders, but workers as well. It is clear that the challenge of today's professionals is to prepare their companies and leaders for change. For example, I feel that Mexican organizations are using leadership training in change management as a primary means of meeting this challenge—considering that the most commonly cited means of increasing productivity is through improved leadership.

# ARE YOU A GOGETEMITE?



**gogetemite** n. (2007):  
an enthusiastic professional eager  
to make bold changes to his or  
her career.

**Example:** Today the gogetemite  
called Lander International to  
jumpstart his/her career.

Speak today with a Lander International Recruiting Coach to build your marketable skills for the job market of the future. Lander International has been helping place IT auditors into the most progressive internal audit and consulting organizations for the last 29 years. Visit [www.landerint.com](http://www.landerint.com) to meet the Lander International team and read testimonials from gogetemites.

**LANDER**  
INTERNATIONAL, LLC

*Because your search is THAT important*

(800) 548-5318 in USA and Canada  
(510) 232-4264 International  
[www.landerint.com](http://www.landerint.com)



# ISO 27001 Training

## ISO 27001 Lead Auditor

The ISO27001 Lead Auditor course provides you with the knowledge necessary to perform an audit or take charge in the auditing of an ISMS, information security management system.

The five day intensive course is based on the ISO 19011:2002 standard and other international audit standards and guidelines, and is conceived specifically for those who wish to carry out external or internal audits according to the ISO 27001:2005 standard's criterion.



Certified by the RABQSA

## ISO 27001 Implementation

The ISO 27001 Information Security Management Systems (ISMS) Implementation course teaches students the necessary steps of ISMS implementation as specified in ISO 27001.

The training is also aligned with best practices with regards to project management according to the Project Management Institute (PMI) and the International Project Management Association (IPMA) as well as the ISO 10006 standard, "Guidelines for quality management in project".



### United States

Anaheim	Las Vegas
Atlanta	Los Angeles
Boston	New York
Buffalo	San Diego
Chicago	San Francisco
Dallas	Seattle
Detroit	Tampa
Houston	Washington

### International

Alger	Mexico
Beijing	Montreal
Bogota	Paris
Buenos Aires	Quito
Bucharest	Santiago De Chile
Casablanca	Toronto
Lima	Vancouver
Madrid	Victoria

1-866-949-2088

[training@veridion.net](mailto:training@veridion.net)



**VERIDION**

© 2007 Veridion Inc.

[www.veridion.net](http://www.veridion.net)



# Stepping Through the InfoSec Program

By J. L. Bayuk, CISA, CISM

Review by C. Warren Axelrod, Ph.D., CISM, CISSP

This is the author's second "Stepping Through..." book. The first book, *Stepping Through the IS Audit*, was written to help both auditors and auditees through the intricacies of the information systems (IS) audit process. The second book, *Stepping Through the InfoSec Program*, tackles the broader and, in some ways, more challenging topic of establishing and running an information security program.

Although the second book is clearly directed at the information security manager, it could provide value to a number of constituencies. For one, IS auditors may find the book useful as a basis for determining what an ideal information security program should be. Business unit managers may benefit greatly from this book, particularly when dealing with the information security group, and less-technical readers will find the case study helpful to understand the key aspects of an information security program in operation.

While the covers of both books show three smiling professionals walking through a barrier of zeros and ones, Stargate style, most novices and many experienced security professionals likely envision the process of setting up and executing an information security program to be more like making their way cautiously through a minefield. Unfortunately, the latter description may indeed be more representative of the experience for many organizations as well. Consequently, the primary need is for no-nonsense, to-the-point guidance to establish and enforce an information security program; this is what the book provides so well.

If my experience is typical, the information security professional tasked with setting up an information security program starts out by writing policy. Once the security policy and standards have been dutifully copied from one of the many available sources, what should be done next? Without a realistic guide to the next steps, information security professionals may find themselves at a loss. This book is one such guide and can help professionals get over the hurdle.

*Stepping Through the InfoSec Program* consists of three sections: the context in which information security programs are developed, the components of the information security program itself and a case study in the form of a chatty but substantive dialog. Notably, the first part focuses on individuals, whereas the second and third parts focus on the program.

The first part provides a comprehensive background and a practical context, including:

- A description of the history leading up to today's information security programs
- An enumeration of the various job functions that relate to information and physical security

- Descriptions of the roles and responsibilities of those within the various functions
- A list of respected certifications in the field
- A discussion of metrics used to determine performance of the information security function

The second part presents the components of an information security program. It guides the reader through the following:

- Creation of the information security program
- Relating the information security program to information technology governance
- Ensuring accountability through roles and responsibilities
- Identification and location of resources to achieve objectives
- Determination that the program is meeting objectives

Because this second part is so full of information, issues and advice, it may require careful reading and rereading to internalize some of the most critical areas, but it is well worth the effort. Having conquered the concentrated information in the second part, the reader may find it to be somewhat of a relief to move into the third part, the case study.

The case study brings home the many lessons of the second part in a lighter, more readily digestible form. One gets the impression from the keenly crafted scenes that the author has actually lived through many of the scenarios described. This incorporation of dialog, which is a technique that was also used in the first book, is unusual for books of this type, but works well in reiterating the many concepts previously presented.

Following the three sections that comprise the body of the book are a number of useful appendices. Sample policy, standard, procedure and guideline documents are included. These serve not only as examples, but are also valid documents that could be used directly.

## C. Warren Axelrod, Ph.D., CISM, CISSP

is the business information security officer and chief privacy officer for United States Trust Company, N.A. At US Trust, he identifies, assesses and mitigates privacy and security risks, and ensures that employees are familiar with privacy and security policy and procedures. Axelrod is involved in the financial industry and with cybersecurity and critical infrastructure issues at the national level.

## Editor's Note:

*Stepping Through the InfoSec Program* is available from the ISACA Bookstore. For information, see the ISACA Bookstore Supplement in this *Journal*, visit [www.isaca.org/bookstore](http://www.isaca.org/bookstore), e-mail [bookstore@isaca.org](mailto:bookstore@isaca.org), or telephone +1.847.660.5650.



# Information Development: Managing Your Documentation Projects, Portfolio, and People

By JoAnn T. Hackos, Ph.D.

*Reviewed by Soumen Chatterjee*

Information is the driving force of the rapidly growing enterprise economy. However, it is also one of the most misunderstood intangible assets. Information, including information technology, is often ignored in traditional enterprise. Douglas W. Hubbard of Hubbard Decision Research has created a revolutionary methodology called Applied Information Economics, which shows how information should be scientifically measured. However, information development is always the first step, and this rare art is presented in *Information Development: Managing Your Documentation Projects, Portfolio, and People* by JoAnn T. Hackos. This book is a timely contribution to the information age. It is divided into three parts: the framework, portfolio management and project management.

Part one of this book describes the information process maturity model (IPMM). Eleven chapters are dedicated to portfolio management and 11 more chapters describe the art of project management. Altogether, the book contains 24 chapters and is based on the author's knowledge gained throughout her 25 years of industry experience.

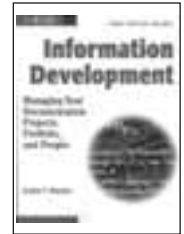
Another highlight of the book is its inclusion of tables. Tables 2-1 and 2-4 describe the IPMM, collaboration key characteristics and change management key characteristics. Table 9-2 describes a different perspective of tool selection that highlights several important categories of tools such as authoring, controlled language, review and collaboration, metadata and taxonomy, production (print, help systems, web content and interactives), graphics, content management (component, document, document management and web content management), translation, and search and retrieval. Table 16-8 highlights project dependencies, which include product stability and completeness, information availability, prototype availability, subject matter expert availability, review experience, technical experience, writing and design experience, audience understandability, team experience, and tools experience.

One of the most important messages that the author successfully explains in this book is portfolio management. Information is one of the greatest assets in any organization's portfolio, and the book successfully explains why the portfolio is so critical, outlines its benefits and describes best practice guidelines in managing a strategic portfolio.

This book should be considered by experienced professionals who are engaged in information development projects and activities. However, it may also be useful for beginners who are interested in increasing their awareness about information value.

*Information Development: Managing Your Documentation Projects, Portfolio, and People* can be used by professionals in any enterprise industry, including, but not limited to, information technology, financial services, manufacturing, telecommunications, healthcare, government, banking, insurance and education.

Additionally, the book contains a strong bibliography for those who want to take on further study or research.



## **Soumen Chatterjee**

is an enterprise architect for a UK-based global leading consulting company and is a TOGAF Certified Practitioner, Sun Certified Enterprise Architect and IBM Certified Specialist in Rational Unified Process (RUP). With his expertise in enterprise architectural methodologies, process development techniques and testing strategies, he has served several leading-edge software service organizations. He has published several technical papers in architecting journals and Internet-based publication portals.

## **Editor's Note:**

*Information Development: Managing Your Documentation Projects, Portfolio, and People* is available from the ISACA Bookstore. For information, see the ISACA Bookstore Supplement in this *Journal*, visit [www.isaca.org/bookstore](http://www.isaca.org/bookstore), e-mail [bookstore@isaca.org](mailto:bookstore@isaca.org), or telephone +1.847.660.5650.

## CACS CONFERENCES

**Asia-Pacific CACS<sup>SM</sup>**

For more information  
on this event, please visit  
[www.isaca.org/asiacacs](http://www.isaca.org/asiacacs).

**EuroCACS<sup>SM</sup>**

For more information  
on this event, please visit  
[www.isaca.org/eurocacs](http://www.isaca.org/eurocacs).

**North America CACS<sup>SM</sup>**

For more information  
on this event, please visit  
[www.isaca.org/nacacs](http://www.isaca.org/nacacs).

**Latin America CACS<sup>SM</sup>**

Santiago, Chile  
17-20 August 2008  
[www.isaca.org/latincacs](http://www.isaca.org/latincacs)

**Oceania CACS<sup>SM</sup>**

Sydney, New South Wales, Australia  
8-10 September 2008  
[www.isaca.org/oceaniacacs](http://www.isaca.org/oceaniacacs)

## INTERNATIONAL CONFERENCE

**International Conference**

Toronto, Ontario, Canada  
27-30 July 2008  
[www.isaca.org/international](http://www.isaca.org/international)

## SECURITY CONFERENCES

**Information Security Conference  
(Latin America)**

For more information on this event, please visit  
[www.isaca.org/infosecuritypanama](http://www.isaca.org/infosecuritypanama).

**Network Security Conference**

Las Vegas, Nevada, USA  
8-10 September 2008  
[www.isaca.org/nsc](http://www.isaca.org/nsc)

**Information Security  
Management Conference**

Las Vegas, Nevada, USA  
8-10 September 2008  
[www.isaca.org/infosecurity](http://www.isaca.org/infosecurity)

**Network Security Conference (Europe)**

Amsterdam, The Netherlands  
10-12 November 2008  
[www.isaca.org/nsc](http://www.isaca.org/nsc)

**Information Security  
Management Conference (Europe)**

Amsterdam, The Netherlands  
10-12 November 2008  
[www.isaca.org/infosecurity](http://www.isaca.org/infosecurity)

## IT GOVERNANCE EDUCATION

**IT Governance, Risk and Compliance Conference**

Orlando, Florida, USA  
8-10 October 2008  
[www.isaca.org/itgrc](http://www.isaca.org/itgrc)

**IT Governance Forum**

Scottsdale, Arizona, USA  
27-28 October 2008  
[www.isaca.org/managementforums](http://www.isaca.org/managementforums)

## MANAGEMENT FORUMS

**IT Audit Management Forum**

Scottsdale, Arizona, USA  
27-28 October 2008  
[www.isaca.org/managementforums](http://www.isaca.org/managementforums)

**Information Security  
Management Forum**

Scottsdale, Arizona, USA  
27-28 October 2008  
[www.isaca.org/managementforums](http://www.isaca.org/managementforums)

**IT Audit Management Forum (Europe)**

Zurich, Switzerland  
13-14 November 2008  
[www.isaca.org/managementforums](http://www.isaca.org/managementforums)

## COBIT EDUCATION

**COBIT<sup>®</sup> User Convention**

For information on attending or  
hosting an event, please visit  
[www.isaca.org/cobituserconvention](http://www.isaca.org/cobituserconvention).

**Using COBIT<sup>®</sup> in IT Audit**

(classroom)  
[www.isaca.org/cobiteducation](http://www.isaca.org/cobiteducation)

**COBIT<sup>®</sup> Awareness Course**

(online)  
[www.isaca.org/cobitcampus](http://www.isaca.org/cobitcampus)

**COBIT Foundation Course<sup>™</sup>**

(online and classroom)  
[www.isaca.org/cobitcampus](http://www.isaca.org/cobitcampus)

**Implementing IT Governance  
Using COBIT<sup>®</sup> and Val IT<sup>™</sup>**

(classroom)  
[www.isaca.org/cobitcampus](http://www.isaca.org/cobitcampus)

**COBIT<sup>®</sup> for Sarbanes-Oxley  
IT Compliance Course**

(online)  
[www.isaca.org/cobitcampus](http://www.isaca.org/cobitcampus)

## SYMPOSIA

**IT Controls for Sarbanes-Oxley:  
The Symposium**

[www.isaca.org/soxsymposium](http://www.isaca.org/soxsymposium)  
Rosemont, Illinois, USA  
19-20 June 2008  
Washington DC, USA  
15-16 September 2008  
Dallas, Texas, USA  
4-5 December 2008

**IT Control Objectives for Basel II**

[www.isaca.org/baselsymposium](http://www.isaca.org/baselsymposium)  
Las Vegas, Nevada, USA  
1-2 May 2008  
Toronto, Ontario, Canada  
31 July 2008  
Zurich, Switzerland  
12 November 2008



## ISACA TRAINING WEEK

[www.isaca.org/trainingweek](http://www.isaca.org/trainingweek)

Dallas, Texas, USA  
7-11 April 2008

Vancouver, British Columbia, Canada  
9-13 June 2008

Minneapolis, Minnesota, USA  
23-27 June 2008

Edinburgh, Scotland, UK  
15-19 September 2008

Washington DC, USA  
22-26 September 2008

Anaheim, California, USA  
8-17 October 2008

Chicago, Illinois, USA  
3-7 November 2008

New Orleans, Louisiana, USA  
8-12 December 2008

## CISA REVIEW

**CISA<sup>®</sup> Online Review Course**

For information on this course,  
please visit [www.isaca.org/cisareview](http://www.isaca.org/cisareview).

## E-SYMPOSIA AND WEBCASTS

For information on webcasts and  
monthly e-symposia, please visit  
[www.isaca.org/webcasts](http://www.isaca.org/webcasts).

Coming  
Soon!



SARBANES-OXLEY  
SYMPOSIUM



# A Prelude to IT Assurance Framework

By Ravi Muthukrishnan, CISA, CISM, FCA

*"Necessity is the mother of invention."*

—Plato, Greek philosopher

One of the single most important issues on the agenda of senior executives and boards today is the effectiveness of internal controls on information technology (IT). With IT becoming more pervasive, technology-based solutions are increasingly replacing manual processes. In addition, to meet the expectations and demands for the right information from shareholders, regulators and other stakeholders, it is critical for automated internal controls to be effective and efficient. This places added onus and great responsibility on assurance professionals to ensure quality, objectivity, consistency and reliability of their IT control assessments.

ISACA's IT Assurance Framework™ (ITAF™) is designed to meet the continuing need of IT assurance professionals by providing a framework, direction and a single point of reference to host standards, guidelines, tool and techniques to conduct IT assessments. This comprehensive framework for IT audit and assurance professionals is the vision of Marios Damianides, CISA, CISM, CA, CPA, a past international president of ISACA, and was spearheaded by Robert Parker, CISA, CA, CMC, FCA, also a past international president of ISACA. ITAF is a result of their shared passion, and came about only after many hours of effort over two years.

The challenge and goal were to create a comprehensive "one-stop" framework for IT audit and assurance professionals.

## What Is ITAF?

ITAF is a comprehensive and good-practice-setting framework that:

- Provides guidance on the design, conduct and reporting of IT audit and assurance assignments
- Defines terms and concepts specific to IT assurance
- Establishes standards that address IT audit and assurance professional roles and responsibilities, knowledge and skills, diligence, conduct, and reporting requirements

The current version of ITAF, published in *ITAF™: A Professional Practices Framework for IT Assurance*, incorporates existing standards and guidelines of ISACA. The framework allows for new guidance to be indexed properly as it is developed and issued. Designed to be a living document, ITAF is flexible and allows for material such as relevant tools, techniques, white papers and publications to be placed within the framework—in addition to standards and guidelines.

## ITAF Development

The ITAF project, approved by the ISACA Board of Directors in 2006, was originally conceptualized to address only audit and assurance standards, as that is where the greatest need had been identified. As the IT audit and assurance standards were developed and the project matured, additional needs were identified, including the development of the ITAF taxonomy to encompass the body of knowledge with which the IT audit and assurance professional must be aware. Accordingly, the initial taxonomy was designed and presented to ISACA's Assurance Committee and Standards Board in late 2006. Since then, ITAF has been subjected to a variety of input and due diligence processes. Throughout these processes the issues raised and guidance provided by members of the IT audit and assurance profession have proven invaluable in establishing scope, content and direction.

ITAF is a living document. It will evolve as business, technology and assurance practices evolve. It is a document for the profession and will continue to solicit and value the input provided by its constituents and stakeholders.

## Who Should Use ITAF?

ITAF is designed primarily for use by individuals who act in the capacity of IT audit and assurance professionals and are engaged in providing assurance over some components of IT systems, applications and infrastructure; however, it can be used by anyone in the assurance profession. The framework is designed to provide benefits to wider audiences including senior management, boards, and users of IT and assurance reports.

ITAF's design recognizes that IT professionals are faced with multiple requirements and types of audit, ranging from IT-focused audit to financial, operational or regulatory requirements. At this time, ITAF is not designed to address specific requirements with respect to consultative and advisory work.

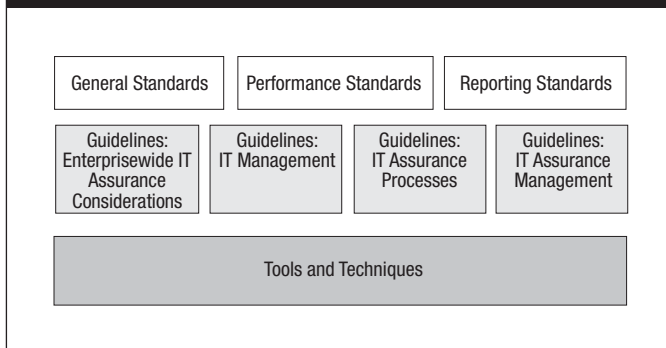
## How Is ITAF Organized?

Figure 1 illustrates the basic components of ITAF. These include three categories of standards—general, performance and reporting—as well as guidelines and, finally, tools and techniques:

### • Standards:

- General—These are the guiding principles under which the IT assurance profession operates. These apply to the conduct of all assurance assignments, and deal with the IT audit and assurance professional's ethics, independence, objectivity and due care as well as knowledge, competency and skill.

**Figure 1—ITAF Hierarchy**



- Performance—These standards deal with the conduct of the assignment such as planning and supervision, scoping, risk and materiality, resource mobilization, supervision and assignment management, audit and assurance evidence, and the exercising of professional judgment and due care.
- Reporting—These standards address the types of reports, means of communication and the information communicated.
- **Guidelines**—These provide the IT audit and assurance professional with information and direction about an audit or assurance area in line with the three categories of standards. Guidelines focus on the various audit approaches, methodologies and related material to assist in planning, executing, assessing, testing and reporting on IT processes, controls, and related audit or assurance initiatives. Guidelines also help clarify the relationship between enterprise activities and initiatives, and those undertaken by IT.
- **Tools and techniques**—These provide specific information on various methodologies, tools and templates, and direction in their application and use, to operationalize the information provided in the guidance. The tools and techniques are directly linked to specific guidelines. They take a variety of forms, such as discussion documents, technical direction, white papers, audit programs or books, e.g., the ISACA publication *Security, Audit and Control Features SAP® R/3®, 2<sup>nd</sup> Edition: A Technical and Risk Management Reference Guide*, which supports the guideline on enterprise resource planning (ERP) systems.

Due to the diverse global requirement, ITAF has recognized the use of standards established by other global and national standard-setting bodies. As a result, IT audit and assurance professionals may use ISACA standards in conjunction with professional standards issued by other authoritative bodies. It also describes how to deal with inconsistencies, if any, with other standards.

ITAF is divided into four sections:

- **1000**—Provides an introduction to ITAF, discusses how to use it, describes the audience and introduces the ISACA Code of Professional Ethics
- **2000**—Presents the three categories of standards: general, performance and reporting
- **3000**—Introduces the guidelines. In this section, tables provide information in two categories:
  - IT processes or IT audit processes—Includes a narrative description of the guideline item, presents information

about the subject area and the assurance issues, and provides direction to IT audit and assurance professionals.

– Resources—Provides references to:

- ISACA resources—A list of existing ISACA IS Auditing Standards, IS Auditing Guidelines, and other ISACA and IT Governance Institute (ITGI) publications relevant to the subject matter
- Other resources—A list of relevant material from other standards-setting or regulatory bodies considered appropriate to the guideline's subject matter
- **4000**—Establishes the IT audit and assurance tools and techniques as well as other information such as discussion documents, technical direction, white papers, audit programs or detailed books, that provide IT audit and assurance professionals with the detailed guidance needed to accomplish their mission. (This section is in development and will be introduced gradually.)

In line with ITAF's design as a living document, section numbers intentionally include gaps where future information may be inserted. **Figure 2** describes how the four sections of ITAF are organized.

## Adopting ITAF

The IT assurance or audit process involves the conduct of specific procedures to provide an appropriate level of assurance about the subject matter. IT audit and assurance professionals undertake assignments designed to provide assurance at varying levels, ranging from review to attestation or examination.

Several critical hypotheses are inherent in any IT assurance or audit assignment, including the following:

- The subject matter is identifiable and subject to audit.
- The audit or assurance project, if undertaken, has a significant likelihood of successful completion.
- The audit or assurance approach and methodology are free from bias.
- The IT audit or assurance project is of sufficient scope to meet the audit or assurance objectives.
- The IT audit or assurance project will lead to a report that is objective and will not mislead the reader.

Some of the salient features of ITAF that IT audit and assurance professionals may want to consider in adopting it are:

- Important terms and definitions in section 1800
- Classification and explanation of the level of assurance in section 1800
- Reference to general standards in section 2200
- Reference to performance standards in section 2400
- Reference to reporting standards in section 2600, e.g., **figure 3**, which specifies the types of reports based on user needs
- Section 3000's detailed references to IT processes, with corresponding mapping to available ISACA and other resources. IT processes are comprehensive and easily understandable. Resources include mapping to appropriate guidelines, COBIT and other publications of ISACA/ITGI. This information is highly valuable to IT assurance professionals seeking a one-stop reference point for their guidance, assistance on types of engagements and an overall framework for their profession.

**Figure 2—ITAF Sections**

Section	Subsection	Description
<b>Section 1000—Introducing the IT Assurance Framework</b>		
1100		ITAF: A Brief Overview
1500		Organization of the IT Assurance Framework
1700		Use of the IT Assurance Framework
1800		Important Terms and Definitions
1900		How This Publication Is Organized
<b>Section 2000—IT Assurance Standards: Defining a Common Reference Point</b>		
2100		IT Assurance Standards: Overview and Use
	2150	Code of Professional Ethics
2200		General Standards
2400		Performance Standards
2600		Reporting Standards
<b>Section 3000—IT Assurance Guidelines: Putting the Standards Into Practice</b>		
3100		IT Assurance Guidelines: Overview and Use
3200		Enterprise Topics
	3210	Implication of Enterprisewide Policies, Practices and Standards on the IT Function
	3230	Implication of Enterprisewide Assurance Initiatives on the IT Function
	3250	Implication of Enterprisewide Assurance Initiatives on IT Assurance Plans and Activities
	3270	Additional Enterprisewide Issues and Their Impact on the IT Function
3400		IT Management Processes
	3410	IT Governance (Mission, Goals, Strategy, Corporate Alignment, Reporting)
	3412	Determining the Impact of Enterprise Initiatives on IT Assurance Activities
	3415	Using the Work of Other Experts in Conducting IT Assurance Activities
	3420	IT Project Management
	3425	IT Information Strategy
	3427	IT Information Management
	3430	IT Plans and Strategy (Budgets, Funding, Metrics)
	3450	IT Processes (Operations, Human Resources, Development, etc.)
	3470	IT Risk Management
	3490	IT Support of Regulatory Compliance
3600		IT Audit and Assurance Processes
	3605	Relying on the Work of Specialists and Others
	3607	Integrating IT Audit and Assurance Work With Other Audit Activities
	3610	Using COBIT in the IT Assurance Process
	3630	Auditing IT General Controls (ITGCs)
	3650	Auditing Application Controls
	3653	Auditing Traditional Application Controls
	3655	Auditing Enterprise Resource Planning (ERP) Systems
	3657	Auditing Alternative Software Development Strategies
	3660	Auditing Specific Requirements
	3661	Government-specified Criteria
	3662	Industry-specified Criteria
	3670	Auditing With Computer-assisted Audit Techniques (CAATs)
	3680	IT Auditing and Regulatory Reporting
	3690	Selecting Items of Assurance Interest
3800		IT Audit and Assurance Management
	3810	IT Audit or Assurance Function
	3820	Planning and Scoping IT Audit and Assurance Objectives
	3830	Planning and Scoping IT Audit and Assurance Work
	3835	Planning and Scoping Risk Assessments
	3840	Managing the IT Assurance Process Execution
	3850	Integrating the Audit and Assurance Process
	3860	Gathering Evidence
	3870	Documenting IT Audit and Assurance Work
	3875	Documenting and Confirming IT Audit and Assurance Findings



**Figure 2—ITAF Sections (cont.)**

Section	Subsection	Description
	3880	Evaluating Results and Developing Recommendations
	3890	Effective IT Audit and Assurance Reporting
	3892	Reporting IT Audit and Assurance Recommendations
	3894	Reporting on IT Advisory and Consultancy Reviews
Section 4000—IT Assurance Tools and Techniques (reserved for future development)		

**Figure 3—Types of Reports Based on User Needs**

The Report the User Needs	Consulting Services	Attestation Procedures	Agreed-on Procedures	SAS 70 <sup>1</sup> Section 5970 <sup>2</sup>	Trust Services SysTrust and WebTrust <sup>3</sup>
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

## Conclusion

In reference to the quote of Plato at the beginning of the article, there is a dire need for such a framework for IT audit and assurance professionals; it fills a great void.

Promised to be a living document, it will be interesting to see how this product eventually grows and adopts available technology to make it even more user friendly.

## Reference

ISACA, *ITAF: A Professional Practices Framework for IT Assurance*, USA, 2008

## Endnotes

<sup>1</sup> American Institute of Certified Public Accountants (AICPA), Statement on Auditing Standards (SAS) No. 70, *Service Organizations*, USA

<sup>2</sup> Chartered Accountants of Canada (CICA), Section 5970, Canada

<sup>3</sup> Trust Services (including WebTrust and SysTrust) is a set of professional assurance and advisory services based on a common framework from the AICPA and CICA.

### Ravi Muthukrishnan, CISA, CISM, FCA

is chief financial officer at Capco IT Services, India, and is currently chair of the ISACA Standards Board. He has been working with the Standards Board since 2003 and is an active member of the ISACA Bangalore Chapter. He can be reached at [mravikrishnan@vsnl.com](mailto:mravikrishnan@vsnl.com) or [m.ravi@capco.com](mailto:m.ravi@capco.com).

## ALTERNATIVE?



Including 25 partners and principals, the firm has an experienced team of IT and internal control professionals available to strengthen and/or test IT and business control environments at cost effective rates. Some of the services offered include:

- ▶ SAS 70 audits
- ▶ IT and business controls assessments
- ▶ Section 404 implementation, remediation or maintenance
- ▶ Outsourced internal audit function

For more information:  
**Chris Mitchell**  
 972.788.4467  
[cmitchell@kbagroupllp.com](mailto:cmitchell@kbagroupllp.com)

**KBA**<sup>®</sup>  
 GROUP | LLP  
 Certified Public Accountants  
 ▶ [www.kbagroupllp.com](http://www.kbagroupllp.com)

# Using COBIT 4.1 to Guide the Adoption and Implementation of Open Source Software

By Steven De Haes, Ph.D., Wim Van Grembergen, Ph.D., Kris Ven and Jan Verelst

In the past few years, open source software (OSS) has become a viable solution for organizations. OSS is software that is distributed under a license that complies with the Open Source Definition.<sup>1</sup> This essentially means that the software is free for anyone to download, install, modify and distribute. Although OSS has its roots in a volunteer community, the interest of commercial vendors has increased considerably in recent years. Many organizations have already adopted OSS. One of the main appeals of OSS is that it is available free of charge. On the other hand, research on the adoption of OSS has shown that there are a number of issues that organizations may experience when migrating to OSS. Some authors have developed evaluation frameworks that are specifically targeted toward OSS.<sup>2</sup> However, it is the opinion of this article's authors that it is useful to apply existing frameworks to OSS, such as *Control Objectives for Information and related Technology* (COBIT), since OSS needs to support the same business needs and processes and should meet the same criteria as proprietary software.

Based on available literature, some of the most pertinent issues that may arise during the adoption of OSS are presented in this article. Next, the article illustrates which control objectives and control practices contained in COBIT may prove to be particularly useful in the decision-making process, to mitigate the risks involved in adopting OSS. The aim is to discuss how COBIT can help in adopting OSS in a controlled manner.

## Key Issues in OSS Adoption

Based on a literature review, some of the most important issues in adopting OSS are:

- **OSS as a strategic choice**—The organizational adoption of OSS is still a relatively recent phenomenon. Hence, many decision makers are currently not sufficiently familiar with OSS. In other cases, decision makers may have heard of OSS, but do not further investigate it or have insufficient knowledge on whether the organization could benefit from adopting OSS. In addition, decision makers may have certain prejudices against OSS based on outdated information, and consider OSS to be immature and not suitable for organizational use.<sup>3</sup> On the other hand, some organizations try to use OSS whenever possible in the organization.
- **External support**—Research has shown that the availability of consultancy and external support is a major enabler for the adoption of OSS.<sup>4,5</sup> Conversely, the lack of support for some OSS products has been shown to be an important barrier for the adoption of OSS. No official support is

available for OSS that is downloaded over the Internet. Although user assistance is provided through online channels such as mailing lists, forums or wikis, (corporate) users have no assurance that they will be provided with accurate and timely assistance for any problems they experience. For business-critical systems, the support offered by the OSS community is likely to be insufficient and professional support is required. Several vendors offer commercial versions of OSS that include professional support services. The most well-known examples are the enterprise Linux versions of Red Hat and SUSE. Many OSS vendors have certified local representatives to ensure that organizations can contact a nearby service provider. Other third parties provide assistance in selection, implementation and maintenance.

- **Cost considerations**—OSS can be downloaded from the Internet free of charge. However, studies have shown that the real cost benefits of using OSS are difficult to assess.<sup>6</sup> In general, organizations have no clear idea whether the total cost of ownership (TCO) of OSS is lower than the TCO of proprietary software. Although many studies have compared the TCO of OSS and proprietary solutions, it remains difficult to generalize these results. The unclear outcome of the TCO for an OSS solution can be explained by a number of factors. First, implementing commercial OSS is not free of charge because a fee is due for the support contract. Second, it has been shown that the introduction of OSS implies additional costs for training, migration and maintenance.<sup>7</sup> Finally, the context of the organization is important in calculating a TCO.<sup>8</sup> Hence, the cost advantage of OSS compared to proprietary solutions may be less than could be expected.
- **Skilled information technology (IT) staff**—The current skills of the IT staff are an important aspect in the adoption decision on OSS. Research has shown that depending on the skills and experience of the IT staff, the migration can prove to be rather difficult (and thus expensive).<sup>9</sup> For example, the migration from a UNIX-based infrastructure to Linux is, in general, easier than a migration from a Microsoft Windows-based platform to Linux. This is caused by the fact that UNIX and Linux are closely related, and many of the administrative tools are shared. Hence, IT staff members who are familiar with UNIX experience fewer problems when confronted with a Linux system; IT staff members with a background in MS Windows experience substantially more difficulties in adapting to Linux.
- **Training users**—Replacing proprietary software with OSS can be a disruptive change for users in the organization. The

impact on the organization mainly depends on the type of software that is adopted. If OSS is adopted for infrastructure software (e.g., operating systems, web servers, mail servers), the impact is limited to IT staff members since end users do not interact directly with those systems. However, the adoption of OSS on desktop computers is noticeable by almost all users in the organization. Retraining users may represent a considerable investment, as users may have a long experience working with proprietary software, even outside the workplace. Nevertheless, several organizations have already migrated successfully toward OSS on the desktop, including the use of Linux, Mozilla Firefox and OpenOffice.org. Research on these migrations has shown that it is important that users receive proper training.<sup>10</sup> Training can help users to see the differences and adjust their working habits. Another finding from research indicates that it is important to create a favorable attitude with end users toward the OSS solution, e.g., by informing users about the migration.<sup>11</sup>

- **Implementation**—The implementation of OSS in the organization has a number of specific characteristics. Researchers have studied how OSS can be implemented successfully in organizations.<sup>12</sup> This article focuses on a number of important findings. Studies on the migration to OSS have recommended conducting a pilot study before commencing a full-scale migration.<sup>13</sup> This helps in identifying potential problems and solutions and ensures that the migration progresses smoothly. It can also function as a feasibility study that can support the decision on whether to continue with a full-scale migration.

An interesting characteristic of OSS is that it provides access to the source code of the software. Proponents of OSS claim that the availability of the source code is one of the main advantages of OSS, as everyone can read and improve the software. On the other hand, many studies have shown that most organizations never actually make use of the source code.<sup>14</sup> This can be explained by the fact that considerable effort can be required to understand and modify the source code of complex programs such as Linux. In addition, most OSS adopted by organizations is mature software, for which there is little need to modify the source code. However, if the organization uses OSS as building blocks for applications that are developed in-house, the source code may provide useful insight into the inner workings of the program and assist in locating errors in the custom-developed software. In addition, the source code's availability guarantees that the organization can further maintain the software even if the OSS product is no longer maintained.

Finally, OSS generally follows a fairly quick release schedule. The Fedora Linux distribution, for example, includes cutting-edge developments and releases a new version of the operating system every six to nine months. This also means that it may require more effort to maintain OSS systems. Other Linux distributions such as Debian and Red Hat tend to be more conservative, prefer stability over new features, and release a new major version every two to three years.

## Application of COBIT to OSS

Based on the six key issues noted previously for the migration toward OSS, relevant COBIT processes and the subprocesses that can be especially useful when adopting and implementing OSS have been identified as follows. The application of COBIT to OSS adoptions should help in addressing the aforementioned issues and, thus, allow for the OSS adoption in a more controlled manner.

COBIT, from the IT Governance Institute (ITGI), is a freely available good practices framework that originated in the mid-1990s; its latest release, 4.1, was published in 2007. COBIT describes a set of good practices for management, control and security of information technology, and organizes them around a logical framework of 34 IT processes. COBIT 4.1 contains several new important concepts, such as the alignment of business and IT goals, their relationship with supporting IT processes, roles and responsibilities within IT processes, and the interrelationship between IT processes.

**Figure 1** provides an overview of the mapping of COBIT with the six identified key issues of OSS. Only the most relevant control objectives are retained and discussed here. The COBIT control objectives are divided into four domains: Plan and Organize (PO), Acquire and Implement (AI), Deliver and Support (DS), and Monitor and Evaluate (ME). The following breaks down each COBIT process and its relation to OSS adoption.

### *OSS as a Strategic Choice*

- **PO 1.4 IT strategic plan**—Organizations may consider it a strategic choice to base their IT infrastructure on OSS as much as possible. For example, organizations may choose OSS in an effort to reduce vendor lock-in.
- **PO 3.1 Technological direction planning:**
  - OSS can be considered in future decisions as an alternative to proprietary software. Some organizations—especially public administrations—have already proposed guidelines that at least one OSS alternative must be considered when making new IT investments. This ensures that the organization does not miss any opportunities from using OSS.
  - A strengths, weaknesses, opportunities and threats (SWOT) analysis for OSS can be made, based on the specific environment of the organization. A SWOT analysis helps to get insight into the potential benefits of OSS for the organization.
  - Decision makers should take into account which adopter profile the organization wants to follow (i.e., early adopter vs. late adopter). Organizations with a low risk profile should follow a late-adopter strategy. In considering the risk, it is important to take the type of software into account; that is, infrastructure OSS is in general more mature, while enterprise OSS (such as enterprise resource planning [ERP] and customer relationship management [CRM] software) is still a very recent phenomenon.
  - OSS should fit within the enterprise architecture and should be compatible with the overall IT infrastructure. If not, the migration would require too much time and financial resources, and reduce the benefits of adopting OSS.



**Figure 1—Mapping of COBIT With OSS Key Issues**

	Strategy	External Support	Cost Considerations	Skills IT Staff	Training Users	Implementation
PO 1.4 IT Strategic plan	X	X				
PO 3.1 Technological direction planning	X	X				
PO 3.3 Monitor future trends and regulations	X	X				
PO 4.12 IT staffing				X		
PO 4.15 Relationships		X				
PO 5.1 Financial management framework			X			
PO 7.1 Personnel recruitment retention				X		
PO 7.2 Personnel competencies				X		
PO 7.4 Personnel training				X		
PO 7.5 Dependence on individuals				X		
AI 1.3 Feasibility study and formulation of alternative courses of action				X		
AI 2.5 Configuration and implementation of acquired application software				X		
AI 2.6 Major upgrades to existing systems					X	
AI 3.3 Infrastructure maintenance					X	
AI 4.3 Knowledge transfer to end users					X	
AI 5.3 Supplier selection		X				
AI 7.1 Training					X	
AI 7.3 Implementation plan					X	
AI 7.5 System and data conversion					X	
AI 7.8 Promotion to production					X	
DS 1.1 Service level management framework		X				
DS 1.3 Service level agreements		X				
DS 2.3 Supplier risk management		X				
DS 2.4 Supplier performance monitoring		X				
DS 6.3 Cost modeling and charging			X			
DS 7.1 Identification of education and training needs					X	
DS 7.2 Delivery of training and education					X	
DS 7.3 Evaluation of training received					X	

• **PO 3.3 Monitor future trends and regulations:**

- Skilled IT staff members should regularly monitor the emerging OSS technologies that could be relevant for the organization. These IT staff members should have access to technical journals and OSS user groups.
- Since OSS is distributed under licenses that are fundamentally different from proprietary software, the legal counsel should investigate the implications for the organization. Many open source licenses exist today, some of which are very liberal and impose practically no limitations on the use of OSS by the organization (e.g., the BSD license). Other open source licenses are more restrictive and require that derived versions of the software be released under the same open source license (e.g., the GPL license).

**External Support**

- **PO 4.15 Relationships**—The organization must develop good relationships with those vendors that provide external knowledge on OSS systems. Relevant OSS activities in the organization should be communicated to and coordinated with these external parties.
- **AI 5.3 Supplier selection**—Potential providers that can meet the required level of support ought to be identified. The organization needs to determine if support contracts offered by commercial OSS vendors are acceptable or whether

additional support services from a third-party vendor are desirable. It is recommended to investigate if a list of officially recognized support vendors is available. This can help verify the support vendors that have a thorough knowledge of the OSS product and have easy access to the OSS developers.

- **DS 1.1 Service level management framework**—Decision makers must first determine the requested level of support that is required for OSS. Factors that may influence this choice are the lack of in-house OSS expertise and the importance to the business of the system on which OSS is installed.
- **DS 1.3 Service level agreements**—It is important to ensure that service level agreements (SLAs) are agreed upon with the external party providing support for OSS. The SLA management process should ensure that the SLA objectives are measured, so that they can be reported back to the stakeholders. SLAs should be revised when requirements change.
- **DS 2.3 Supplier risk management**—Organizations need to consider the potential risks involved in relying on small, local firms that offer OSS-related services. It is possible that these organizations may not be able to fulfill their contractual agreements, due to their limited size.
- **DS 2.4 Supplier performance monitoring**—The performance of external parties should be monitored and evaluated. Since new OSS vendors continue to appear on the

market, the organization must regularly benchmark the offering of the current suppliers to those of competing vendors.

### **Cost Considerations**

- **PO 5.1 Financial management framework**—A financial framework for the assessment of the costs and benefits should be in place. This is helpful in comparing the cost of an OSS solution with a proprietary solution. It is important that costs be calculated over the whole life cycle of the project, including possible migration costs.
- **DS 6.3 Cost modeling and charging**—The costs of the IT infrastructure should be charged back to business users. These costs are likely to differ between OSS and proprietary software, and the difference will probably impact the adoption decision.

### **Skills IT Staff**

- **PO 4.12 IT staffing**—IT staffing requirements should be evaluated in light of the OSS solution. Some IT staff members should have good knowledge of the OSS, since this facilitates adoption and implementation.
- **PO 7.1 Personnel recruitment and retention**—The human resources management plan should be updated to include OSS-related skills. This includes identifying relevant OSS skills and updating recruitment and training requirements. For some OSS products, it may still be difficult to find highly skilled and experienced professionals. Therefore, key tasks in the organizations need to be identified, and the availability of these skills on the job market should be investigated. Appropriate measures should be taken related to the recruitment and retention of individuals who possess specific OSS skills.
- **PO 7.2 Personnel competencies**—IT personnel should possess or develop the required OSS competencies. Therefore, organizations should encourage IT staff to obtain the necessary knowledge on OSS and acquire the necessary certifications, such as the Linux Professional Institute (LPI) certification, the Red Hat Certified Engineer (RHCE) and Red Hat Certified Technician (RHCT).
- **PO 7.4 Personnel training**—IT staff members should receive appropriate training on OSS to improve their job performance. Lately, an increasing number of training institutions are offering courses on OSS products.
- **PO 7.5 Dependence on individuals**—The key IT staff members involved in the OSS implementations should share their knowledge with others. A situation where a single individual has OSS skills and experience should be avoided; it is necessary to build documentation to plan for succession and to foresee OSS staff backup.

### **Training Users**

- **AI 4.3 Knowledge transfer to end users**—Users should have access to documentation on the OSS product. For some OSS products, limited documentation is available. Commercial vendors of OSS products generally provide high-quality documentation. Firms that offer training courses may also provide documentation for OSS. It is essential that the availability of good documentation from suppliers be evaluated.

- **AI 7.1 Training**—A training approach should be developed to assist users in making the transition. All affected users should have the opportunity to attend the training sessions. An initial training session, focusing on generic skills rather than product-specific skills, is most efficient for users. In a second phase, shorter training sessions can be provided that focus on specific and more advanced tasks.
- **DS 7.1 Identification of education and training needs**—Following the adoption of OSS, the training plan for affected employees should be revised to include the necessary OSS-related skills.
- **DS 7.2 Delivery of training and education**—Sufficient training sessions on OSS should be organized shortly before or after the migration. It is recommended that all users attend this training session, as it has been shown that users who do not follow the training experience meet with more issues after the migration.
- **DS 7.3 Evaluation of training received**—The effectiveness of the training sessions should be assessed by testing the users' knowledge. Possible gaps in the knowledge required for performing tasks should lead to a revision of the training approach or result in additional training sessions.

### **Implementation**

- **AI 1.3 Feasibility study and formulation of alternative courses of action**—Conducting a pilot project in a limited setting before commencing a full-scale migration is recommended. The results from a pilot project are extremely useful for the full-scale migration and may provide more insight into the feasibility of the migration.
- **AI 2.5 Configuration and implementation of acquired application software**—OSS must be configured and implemented to meet the IT and business objectives. Since the source code is available, it is possible to apply modifications. If a third party applies modifications to an OSS used in the organization, an escrow contract providing the safekeeping of the source code is recommended to mitigate the risk of failure of the supplier.
- **AI 2.6 Major upgrades to existing systems**—If the introduction of OSS constitutes a major change in the IT infrastructure (e.g., the migration from Microsoft Windows to Linux), the impact of this change should be properly assessed.
- **AI 3.3 Infrastructure maintenance**—New versions of OSS products can be released more frequently than proprietary software. Therefore, maintenance procedures should state which types of updates and upgrades are applied. Organizations may also prefer OSS that follow a less rapid release schedule to minimize maintenance efforts.
- **AI 7.3 Implementation plan**—An implementation plan that details the different steps in the migration, as well as their interdependencies, should be in place. All affected parties (including external vendors) should be informed about this plan.
- **AI 7.5 System and data conversion**—It is essential to create a system and data conversion plan. In some cases, OSS products include import/export filters for proprietary file formats (e.g., OpenOffice.org is able to read and write most Microsoft Office documents). If the organization primarily uses proprietary formats that are not recognized by the OSS product, data conversion may be difficult and expensive.

- **AI 7.8 Promotion to production**—A formal plan that details how the OSS system should be placed into production must exist. This may also have an impact on supporting activities such as backup and contingency.

## Conclusion

This article has described some key issues that require attention during the adoption and implementation of OSS. Based on these points of interest, a number of COBIT 4.1 control objectives from the PO, AI and DS domains that are particularly relevant for OSS adoption have been identified. In total, 28 of the full 210 control objectives were retained. Of course, it is acknowledged that this selection addressed only the key issues introduced in this paper and that other control objectives are or can be relevant for OSS adoption as well, just as for the adoption of any other proprietary software.

The retained control objectives should help organizations—certainly those that are rather new to OSS—to adopt and implement OSS in a controlled manner. The provided set of control objectives can be leveraged as a quick scan to verify if current management practices in adopting OSS are complete and sufficient for the organization. Similarly, it can help to identify potential improvements in managing the OSS adoption process in the future. Auditors can also use this list of control objectives as a ready-made prescoping when they are confronted with specific assurance assignments in the OSS domain.

COBIT is deemed particularly well suited to improve existing management practices in implementing OSS and to provide assurance over these management practices. The provided subset of control objectives can be a good starting point for supporting these management and assurance activities.

## Endnotes

- <sup>1</sup> Open Source Initiative, “The Open Source Definition,” <http://opensource.org/docs/definition.php>
- <sup>2</sup> Golden, B.; *Succeeding With Open Source*, Addison-Wesley, USA, 2005
- <sup>3</sup> Goode, S.; “Something for Nothing: Management Rejection of Open Source Software in Australia’s Top Firms,” *Information & Management*, 42(5), 2005, p. 669-681
- <sup>4</sup> Ven, K.; J. Verelst; “The Organizational Adoption of Open Source Server Software by Belgian Organizations,” In: Damiani, E.; B. Fitzgerald; W. Scacchi; M. Scotto; G. Succi (eds), *Open Source Systems*, IFIP International Federation for Information Processing, vol. 203, Springer, USA, 2006, p. 111-122
- <sup>5</sup> Dedrick, J.; J. West; “An Exploratory Study Into Open Source Platform Adoption,” Proceedings of the 37<sup>th</sup> Hawaii International Conference on System Sciences, IEEE Computer Society, USA, 2004
- <sup>6</sup> *Ibid.*; *op cit*, Ven 2006
- <sup>7</sup> *Ibid.*
- <sup>8</sup> *Op cit*, Ven 2006
- <sup>9</sup> *Op cit*, Ven 2006 and Dedrick

- <sup>10</sup> Ven K.; D. Van Nuffel; J. Verelst; “The Migration of Public Administrations Towards Open Source Desktop Software: Recommendations From Research and Validation Through a Case Study,” In: Sowe S.K.; I. Stamelos; I. Samoladas (eds); *Emerging Free and Open Source Software Practices*, IGI Publishing, USA, 2007, p. 191-214

<sup>11</sup> *Ibid.*

- <sup>12</sup> *Op cit*, Ven 2006 and Dedrick. Fitzgerald B. and Kenny T. (2003), “Open Source Software in the Trenches: Lessons From a Large-scale Implementation,” In: March T.S.; A. Massey; J.I. DeGross (eds.); Proceedings of the 24<sup>th</sup> International Conference on Information Systems, p. 316-326. Larsen M.H.; J. Holck; M.K. Pedersen; “The Challenges of Open Source Software in IT Adoption: Enterprise Architecture Versus Total Cost of Ownership,” Proceedings of the 27<sup>th</sup> Information Systems Research Seminar, 2004, Scandinavia

<sup>13</sup> *Op cit*, Ven 2007

<sup>14</sup> *Op cit*, Ven 2006 and Dedrick

### Steven De Haes, Ph.D.

is responsible for the information systems management executive programs and research at the University of Antwerp Management School (UAMS) (Belgium). He is managing director of the Information Technology Alignment and Governance (ITAG) Research Institute and recently finalized a Ph.D. on IT governance and business/IT alignment. He has been involved in research and development activities of several COBIT products. He can be contacted at [steven.dehaes@ua.ac.be](mailto:steven.dehaes@ua.ac.be).

### Wim Van Grembergen, Ph.D.

is a professor at the Information Systems Management Department of the University of Antwerp and an executive professor at UAMS. He is academic director of the ITAG Research Institute and has conducted research in the areas of IT governance, value management and performance management. Over the past years, he has been involved in research and development activities of several COBIT products. He can be contacted at [wim.vangrembergen@ua.ac.be](mailto:wim.vangrembergen@ua.ac.be).

### Kris Ven

is currently working at the Information Systems Management Department of the University of Antwerp. He is preparing a Ph.D. on the organizational adoption of OSS. Related research interests include the link between innovation in organizations and OSS, and the adoption of OSS by public administrations. He has written and presented several papers on OSS. He can be contacted at [kris.ven@ua.ac.be](mailto:kris.ven@ua.ac.be).

### Jan Verelst

is professor and vice chair of the Information Systems Management Department at the Faculty of Applied Economics of the University of Antwerp and executive professor at UAMS. His research interests include evolvability of conceptual models and software architectures and OSS. He is a member of the Institute of Electrical and Electronics Engineers (IEEE) and Association for Computing Machinery (ACM). He can be contacted at [jan.verelst@ua.ac.be](mailto:jan.verelst@ua.ac.be).



# Prepare for the 2008 CISM Exams

## ALL NEW—COMPLETELY REVISED—2008 Certified Information Security Manager (CISM) Review Materials for Exam Preparation and Professional Development

To pass the CISM exam, a candidate should have an organized plan of study. To assist individuals with the development of a successful study plan, ISACA offers study aids and review courses to exam candidates (see [www.isaca.org/cismexam](http://www.isaca.org/cismexam) for more details).

### CISM Review Manual 2008

ISACA

The *CISM® Review Manual 2008* has been completely revised and updated with new content to improve consistency and clarity and to remain current in a dynamic field. The updated manual reflects the fact that the information security management profession is rapidly evolving, with increasing responsibilities, scope and authority. Topics covered include governance and management, strategy and policy, security architecture and metrics, and the alignment of security activities with, and in support of, overall business objectives. The new edition also features definitions of terms most commonly found on the exam, practice questions similar in content to what has previously appeared on the exam and references to additional study materials on specific topics. The *CISM Review Manual 2008* is designed to assist candidates in preparing for the CISM exam, and for individuals wanting to learn more about the roles and responsibilities of an information security manager. The 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 2008 edition is organized to help prepare the CISM candidate in 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-8** English Edition  
**CM-8J** Japanese Edition  
**CM-8S** Spanish Edition

### CISM Review Questions, Answers & Explanations Manual 2008

ISACA

The *CISM® Review Questions, Answers & Explanations Manual 2008* consists of 350 multiple-choice study questions that have previously appeared in the *CISM® Review Questions, Answers & Explanations Manual 2007* and the *2007 Supplement*. Many questions have been revised or completely rewritten to recognize a change in job practice, be more representative of the current CISM exam question format, and/or to provide further clarity or explanation of the suggested correct answer. These questions are not actual exam items, but are intended to provide the CISM candidate 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 2008*.

To assist users in maximizing their study efforts, questions are presented in the following two ways:

- Sorted by job practice area
- Scrambled as a sample 200-question exam

**CQA-8** English Edition  
**CQA-8J** Japanese Edition  
**CQA-8S** Spanish Edition

### CISM Review Questions, Answers & Explanations Manual 2008 Supplement

ISACA

Developed each year, the *CISM® Review Questions, Answers & Explanations Manual 2008 Supplement* is recommended for use when preparing for the 2008 CISM exam. Each edition consists of 100 new sample questions, answers and explanations based on the current CISM job practice areas, using a similar process for item development as is used to develop actual exam items. The questions are intended to provide the CISM candidate 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 CISM exam.

**CQA-8ES** English Edition  
**CQA-8JS** Japanese Edition  
**CQA-8SS** Spanish Edition

### CISM Practice Question Database v8

ISACA

The *CISM® Practice Question Database v8* combines the *CISM Review Questions, Answers & Explanations Manual 2008* with the *CISM Review Questions, Answers & Explanations Manual 2008 Supplement* into one comprehensive 450-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 the user's previous scoring history, allowing CISM candidates to easily and quickly identify their strengths and weaknesses, and focus their study efforts accordingly. Other features allow the user to select sample exams by specific job practice areas, view questions that were previously answered incorrectly and vary the length of their study sessions. Also included are *Information Systems Control Journal* articles referenced in the *CISM Review Manual 2008*. The database is available in CD-ROM format or as a web site download.

PLEASE NOTE the following system requirements:

- Intel Pentium 3 or higher (Pentium 4 recommended)
- Windows 98SE or higher
- 256 MB RAM (512 MB recommended)
- Hard drive with 225 MB of available space
- CD-ROM drive
- Display with recommended resolution of 1024 x 768

The CISM Practice Question Database v8 is licensed for installation on one computer only for personal, noncommercial use.

**MDB-8** English Edition—CD-ROM  
**MDB-8W** English Edition—Web site download

**To order CISM® review material for the June or December 2008 exam, see the order form on page S-8 in this *Journal* or visit the ISACA web site at [www.isaca.org/cismbooks](http://www.isaca.org/cismbooks).**

# Keys to Data Governance Success:

## Teamwork and an Iterative Approach

*By Marty Moseley*

**D**ata governance practices are essential for managing data as an asset. These practices establish repeatable, measurable business processes and manageable policies for improving data quality. Data governance helps companies meet regulatory compliance mandates while improving revenue opportunities and customer and partner relationships through the power of higher-quality information.

Despite the universal acceptance that data governance practices are worthwhile, businesses have historically bypassed the discipline in favor of other initiatives that more directly impact the bottom line or provide an immediate return on investment (ROI).

The growing requirements for data privacy and security have altered this landscape for the modern enterprise. Today's commercial businesses are being driven into data governance action by legislation, such as the US Gramm-Leach-Bliley Act and Sarbanes-Oxley Act.

Even with these legislative motivators, data governance is, at best, inconsistent. Most businesses require a guiding hand to assist them with the best ways to achieve success. Once again, companies are discussing the value of data to their corporate operations and attempting to gain insight into corporate performance. However, legislative motivators have created a tipping point where companies must ensure that they are protecting consumer privacy preferences and other personal data.

### Why Companies Struggle

Although some companies today are doing a good job with data governance, they are the exceptions and not the rule. The big question is: why do companies continue to struggle with this practice when the proper management of company data will increase revenue, improve customer and partner relationships and company operations, and assist with regulatory compliance issues?

One reason is that many businesses are shortsighted because they operate on a quarter-by-quarter revenue model. In addition, most publicly traded companies are focused on ensuring strong short-term stock performance. These objectives conflict with data governance initiatives, which usually have a less-direct ROI cycle, and are competing for precious resources with other corporate programs that promise more immediate revenue, efficiency or profitability benefits.

Furthermore, data governance and sharing data among product groups or divisions of the same company can be highly political. Often, business leaders who become territorial about their customer data are unwilling to share data, even for the betterment of the greater good. For instance,

imagine a software company that offers two types of consumer applications. There may be natural relationships between the products, which could afford the company the opportunity to cross-sell to an existing customer base, but the business executive of Division A refuses to share his/her customer data because he/she is not rewarded based on the performance of Division B. This type of "turf war" happens frequently and extinguishes an opportunity for the company as a whole to perform to its best advantage.

A third reason is that most businesses that have tried to implement a data governance practice in their organization have taken the wrong approach. Some companies have tried assigning the program to a single individual who ultimately fails because the job is too big and broad for one person. Still other organizations have knitted together a coalition of interested director-level parties, which has resulted in limited success because this group typically does not have the budget authority needed for a proper data governance program, nor the influence to shift corporate priorities. The most successful initiatives have taken a top-down strategy of appointing an executive sponsor whose "day job" is to get a full understanding of data quality. But, even this approach requires the coordinated efforts of information technology (IT), business management, finance and other functional units such as marketing, product management and sales.

Last, and most important, many companies feel that to achieve data governance success, they must take a "boil the ocean" approach. Trying to tackle all of their data governance issues in one swoop often becomes overwhelming and requires a time investment of several years, with costs escalating before any true return is realized.

### Getting It Together

An effective data governance program includes the people, processes and policies necessary to create a single, consistent view of an enterprise's data. These programs require the coordination of myriad people across organizational and political boundaries, all of whom have other "day jobs." Enlisting senior executives and other employees into a data governance program requires a corporate priority shift, usually away from more "gratifying" tactical issue resolution toward more nebulous and difficult-to-quantify data-quality initiatives.

Instead of employing a top-down, "all or nothing" approach, which requires a complete shift in corporate culture, businesses are better served with an iterative approach to data governance. They should choose a smaller data set, such as customer or product data, and focus their efforts on investigating and fixing it, then determine what worked and

establish policies that can be used to tackle another data set. This more cost-effective, iterative approach enables companies to secure immediate results within months instead of years, while putting into place the scaffolding needed to help manage data quality across all systems. An iterative approach also allows companies to keep an eye on the quarterly revenue ball while making gradual improvements that will ultimately have a favorable impact on the bottom line. It can be thought of as “agile data governance.”

Businesses that combine this bite-size strategy with a strong team approach to data governance are the most successful. The most sensible approach is to appoint a senior executive as committee chair. Ideally, this executive would report directly to the chief executive officer (CEO) and have the clout to dedicate budget, alter corporate priorities and eliminate “turf wars.” The chair should

oversee a board comprised of other executive leaders who have responsibility for each of the company’s lines of business. In addition to this group, an effective data governance team should include individuals representing horizontal functions such as finance, human resources, IT, accounting and marketing; a

---

*An iterative approach  
also allows companies  
to keep an eye on the  
quarterly revenue ball.*

---

group of data experts including a data owner, data steward, data architect and data modeler; and a group of data analysts. The data experts have the following roles and duties:

- **Data owner**—Establishes policies and owns data quality for one or more master data domains, such as customer data, product data, portfolio data and location data
- **Data steward**—Implements and enforces policies and business rules, and corrects data quality problems including matching records, replacing bad data with good data and making “survivorship” decisions if more than one record for the same person exists
- **Data architect**—Evaluates and modifies system components to alleviate data-quality problems
- **Data modeler**—Captures and documents business rules that determine data quality
- **Data analyst**—Discovers and researches problems for the data owner(s) and investigates data quality on a record-by-record, value-by-value basis to look for exceptions, duplicates, etc.

A business can further its success by dovetailing an iterative approach to data governance with some basic committee guidelines. Team members should stay focused on the end result and avoid endless philosophical disagreements about the meaning of data vs. information, the exact definition of an entity or attribute, or what type of representation to use (entity-relationship diagrams or class diagrams). The program will be much more successful if the team can deliver something quickly, even though it might not be 100 percent perfect in its first iteration. The goal of the team should be to complete each iteration rapidly, learn as much as possible, employ a “just enough” process to plan and measure results, make adjustments for the next iteration, and improve the process with each iteration.

## Defining Data Governance Processes

With an iterative approach and the right team in place, commercial businesses are ready to define their data governance processes. These processes typically begin with a business assessment phase and conclude with deployment and ongoing maintenance:

1. **Business assessment**—Articulates various data problems and the value of improving them. This step maps to high-level business processes and helps companies prioritize the pain, issues, costs and value of data. Business assessment results in the definition of the biggest areas of pain, opportunity and risk, and quantifies the value of fixing problems.
2. **Data architecture**—Explains the “ecosystem” in which data are created, maintained, propagated and leveraged for business purposes, and produces a data dictionary and catalog. This step maps data sources and targets, transformation points, moves and transfers (e.g., messages, files), and areas of use in business transactions or decision making. Data architecture results in the measurement of the complexity of the data landscape being examined and influences the definition of the optimal costs and benefits of fixing data.
3. **Proof of concept** (if applicable)—Data governance teams move through steps four, five and six to perform a quick data-quality and remediation process, which includes acquisition, analysis and remediation.
4. **Data acquisition**—Analyzes the data available to select data for transformation. Data acquisition captures data from various sources and produces output for consolidation. At this point, it may be necessary to model data under examination, but enterprises should be careful not to model all of an organization’s data. It is recommended that companies leverage industry standard models or schemas for ideas on how to represent common, highly shared data and map all data taken from source systems to this standard for sharing. This approach keeps system-specific schemas private to systems, while promoting a standard for managing and moving data.
5. **Data analysis**—Profiles source data and models to identify inconsistent or unclear data for clarification and to establish policies and business rules. Data analysis establishes algorithms for determining the uniqueness of data and defines data-quality patterns and business rules for cleansing data. It also creates ongoing procedures for managing data quality, such as triggers, tasks, stakeholders, workflows, processes, approvals and escalations.
6. **Data remediation**—Repairs data according to specified business rules and data-quality processes. Applies business rules’ test results to data, and publishes findings on data-quality results, duplication rates, data error rates and patterns, volumes, and adjustments to data-quality rules.
7. **Evaluation and recommendations**—Produces a final report that evaluates costs, benefits and scope of changes required to alleviate data-quality problems. Determines the implementation phases, expected costs and results, and



finalizes the commitments of the project team to make changes.

8. **Deployment**—Makes systemic, messaging, process and policy changes in participating systems that follow normal development-test-production life cycles. Ensures that systems have migrated to new data values, while protecting data integrity.
9. **Ongoing maintenance**—Evaluates business rules and policies, captures and reports on metrics, and measures progress. Data governance team members may choose to make changes to policies, rules and workflow processes, or may decide to automate something that was once manual, leading back through steps one, two, five, seven and eight.

### Closing Thoughts

Businesses that see the value of a data governance initiative, but are hesitant to begin the process because of concerns about costs or ROI cycles, do not need to abandon their efforts. Instead, they should employ an iterative approach that keeps the scope of the project small and focused on one portion of business data, such as customer or product information. A focused approach enables an organization to realize success quickly, while establishing policies and creating frameworks

that can be applied to other parts of the business in the future. Of course, a successful data governance initiative also requires a strong team, formed from various business leadership positions and strong data resources. Although an incremental approach still requires system changes and results in integration and architectural challenges, companies that choose this route have a much greater chance for success than those that try to “boil the ocean.”

### Marty Moseley

is chief technology officer at Initiate Systems Inc. ([www.initiatesystems.com](http://www.initiatesystems.com)), where he is responsible for the company's strategic technology direction, development and future product evolution. Initiate Systems is a provider of customer-centric master data management software for companies and government agencies that want to create the most complete, real-time views of people, households and organizations from data dispersed across multiple application systems and databases. He can be reached at [mmoseley@initiatesystems.com](mailto:mmoseley@initiatesystems.com).

SERVING IT GOVERNANCE PROFESSIONALS



## Two Conferences in One Location!



### Information Security Management Conference

Providing Strategic Vision  
for Information Security Professionals  
Visit [www.isaca.org/infosecurity](http://www.isaca.org/infosecurity) for details.

### Network Security Conference

Providing the Essentials  
to Secure Your Network  
Visit [www.isaca.org/nsc](http://www.isaca.org/nsc) for details.

8-10 September 2008  
Caesars Palace Las Vegas Resort and Casino  
Las Vegas, Nevada, USA

## Register Now and Save !

Earn up to **32** CPE credits for the event of your choice.

# Auditor Ethics for Continuous Auditing and Continuous Monitoring

*By Jill Joseph Daigle, CISA, CIA, CISSP, Ronald J. Daigle, Ph.D., CPA,  
and James C. Lampe, Ph.D., CPA*

Information technology (IT) auditors within internal audit departments are in a position to add great value to their organizations. Many IT auditors have found that continuous auditing (CA) and continuous monitoring (CM) provide effective control assessments at very low marginal cost. Managers have also quickly recognized the value added by CA and CM. However, a common unrecognized ethical dilemma exists when an IT auditor provides both CA and CM: the potential for losing long-term auditor independence and objectivity because of the different purposes each service has within an organization.

This article describes an occurrence of this dilemma that IT auditors at Amedisys Home Health Services, a publicly traded company with agencies located across the US, faced. The importance of maintaining independence and objectivity, both in fact and appearance, is discussed to show why a potential problem existed at Amedisys. An approach to analyzing the dilemma is presented, as well as the solution implemented by Amedisys, which allowed CA and CM to flourish while maintaining independence and objectivity.

This article reiterates the importance of independence and objectivity and reminds IT auditors that appropriately resolving ethical dilemmas helps reinforce their value to their organizations.

## Implementing a Continuous Audit Initiative

While all had gone well up to this point, the internal audit department of Amedisys had a concern with its CA initiative. Internal audit, including the IT auditors, had been involved with helping meet the section 404 requirements of the US Sarbanes-Oxley Act, i.e., evaluating the system of internal control over financial reporting within their organization. As a result of this process, internal audit recognized that more repetitive and timely IT audit testing of certain key controls, such as CA, would provide more effective and efficient evidence of compliance. As a result, the IT auditors began to identify how CA could be performed in a cost-effective manner.

After careful consideration, Audit Command Language (ACL) was chosen to make CA a reality; automated testing using ACL scripts appeared to provide the ability to efficiently test certain key controls on a recurring basis. The IT auditors sought to identify potential CA opportunities based on risks/benefits, including:

- Identifying terminated users with continued system access
- Identifying dormant accounts of nonterminated users
- Closely monitoring security of critical data
- Identifying duplicate payments to vendors

Prior to considering the use of ACL, Amedisys had met its section 404 compliance needs by establishing a compliance department at the corporate level, assigning a Sarbanes-Oxley manager in the accounting department and assigning Sarbanes-Oxley compliance for IT-related matters to the compliance manager in the IT department. Specific scripts were designed, developed, maintained and used on a recurring basis by the IT auditors, which further assisted with meeting Sarbanes-Oxley compliance.

The ACL scripts were recognized as being so useful for testing key controls that management became interested in using the same or similar scripts for performing CM. The IT department, in particular, took an immediate interest in ACL. The department recognized the benefits of using scripts for its own testing of automated controls and reducing reliance on manual controls. As a result, the IT department made suggestions to improve existing scripts and generated ideas for potential new scripts. The IT auditors used the suggestions to improve the scripts they were maintaining and to create new scripts that they would also maintain, for their own use for CA and for auditee use for CM.

Multiple departments within Amedisys obtained value from the development and maintenance of ACL scripts within internal audit. Internal audit used several scripts for CA and also developed and maintained scripts for CM to help management meet its compliance responsibilities.

So, what was the concern identified by internal audit?

## The Concern

Many business persons, including the IT auditors, saw the scenario described as a win-win situation for all involved. No laws had been broken and persons inside and outside of the organization were better off. However, a serious concern was identified by internal audit at Amedisys; that is, was proper professional judgment being exercised in the application of ethical principles, so that problems down the road may be prevented and the auditors can maximize their long-term value to the organization?

The main point of all accountancy and auditor-related codes of ethics is that key ethical principles must be considered carefully when seeking to make sound professional judgments. Just because no laws are broken or no promulgated rules are violated, does not mean that the most ethically correct behavior is being exhibited. The professional responsibility of an auditor is to consider the ethical principles—the spirit of the rules—that require long-term consideration of the organization and the audit profession, as well as the immediate stakeholders.

All of the professional organizations that provide guidance for auditors and accountants place emphasis on independence and objectivity. A number of these organizations are listed in **figure 1**, along with a respective list of principles or standards. The intent of each list is for professional members of each respective organization to use broad ethical principles to determine the best response to an ethical dilemma.

Note the similarity among the lists of principles; in particular, all five organizations clearly list or imply independence and objectivity as principles that must be adopted and internalized. This emphasis is not just a passing wink at an ethical nicety, but rather the clear recognition that independence and objectivity are core principles and standards that determine the value of a professional's work, especially that of auditors.

Independence and objectivity are emphasized so strongly because when these principles are impaired, so too is the value of an audit. If the user of an audit report does not believe that the auditor is independent and objective, the reliability of information in the audit report is questioned. Therefore, all professional auditors need to be independent in both fact and appearance. ISACA, the Institute of Internal Auditors (IIA) and International Ethics Standards Board for Accountants (IESBA) codes extend the concept further by requiring organizational independence for the internal audit department as well as that of each auditor.

Reflecting back on the scenario at Amedisys, the concern identified by internal audit is justifiably warranted. That is, if ACL scripts are developed and maintained by IT auditors for both their use and the use of management, the IT auditors are being put in the position of auditing their own work. This would result in a clear impairment of both the fact and appearance of the auditor's independence and objectivity, thereby reducing the auditor's value.

## Continuous Auditing Does Not Equal Continuous Monitoring

Despite the previous discussion, some readers still may believe that there is no impairment of auditor independence and objectivity when providing both CA and CM. This false belief may exist because of a misunderstanding of the roles of CA and CM. A difference does exist and it speaks directly to addressing whether auditor independence and objectivity are impaired.

This difference has been identified and emphasized by the ISACA Standards Board.<sup>6</sup> CA and CM may be defined as:

- **CA**—A methodology used by auditors, typically assisted by technology, to perform audit procedures and issue assurance on a continuous basis (e.g., weekly, monthly)
- **CM**—A process put in place by management, usually automated, to determine on a recurring and repetitive basis (e.g., weekly, monthly) if activities are in compliance with policies and procedures implemented by management

Part of what it means for an auditor to be independent and objective is that the auditor cannot audit his/her own work. Associated with this is that an internal auditor cannot audit the work of others for which the internal auditor has ongoing ownership or maintenance responsibilities. CM is a management control function and "the use of continuous monitoring systems by IS auditors may create situations where the IS auditor's independence is impaired."<sup>7</sup>

## The Solution

So, what is the solution to the ethical dilemma facing the IT auditors at Amedisys?

The solution is **not** to find a loophole in an ethics rule that allows the work to be done within the internal audit department.

Rather, the question to be answered is this: How can the IT auditors help management with CM, but also strictly adhere to the principle of maintaining both the fact and appearance of independence and objectivity so that the auditors' work is highly valued?

While there may be no "right" answers that allow a perfect win-win solution for all involved, there are methods that can be used to better understand the consequences of how to react to dilemmas such as those involving CA and CM. First, auditors need to increase their sensitivity to problems that involve ethical principles. Multiple internal auditors with whom the CA vs. CM situation has been discussed had not previously seen a difference between CA and CM. However, upon further discussion and consideration, auditors have recognized that a clear difference does exist between CA and CM, and along with it, a definite threat to the impairment of independence and objectivity.

**Figure 1—Professional Organizations and Respective Guidance Related to Independence and Objectivity**

<i>Professional organization:</i>	ISACA <sup>1</sup>	IIA <sup>2</sup>	Institute of Management Accountants (IMA) <sup>3</sup>	American Institute of Certified Public Accountants (AICPA) <sup>4</sup>	IESBA <sup>5</sup>
<i>Applicable professionals:</i>	IT governance professionals	Internal auditors	Management accountants	Certified Public Accountants (CPAs)	International auditors/accountants
	<ul style="list-style-type: none"> <li>• Objectivity and due care</li> <li>• Honesty and character</li> <li>• Competency</li> <li>• Confidentiality</li> <li>• Compliance with standards</li> <li>• Full disclosure</li> <li>• Professional education</li> </ul>	<ul style="list-style-type: none"> <li>• Objectivity</li> <li>• Integrity</li> <li>• Competency</li> <li>• Confidentiality</li> </ul>	<ul style="list-style-type: none"> <li>• Objectivity</li> <li>• Honesty</li> <li>• Responsibility</li> <li>• Fairness</li> </ul>	<ul style="list-style-type: none"> <li>• Objectivity and independence</li> <li>• Integrity</li> <li>• Due care</li> <li>• Members' responsibilities</li> <li>• Public interest</li> <li>• Scope and nature of services</li> </ul>	<ul style="list-style-type: none"> <li>• Objectivity</li> <li>• Integrity</li> <li>• Competence and due care</li> <li>• Confidentiality</li> <li>• Professional behavior</li> </ul>



Once the problem is identified, the auditor must find the best available solution. A six-step model for helping address ethical dilemmas can be used to identify the best available solution. This model has been widely endorsed by a number of accounting, consulting, journalism, legal, medical and religious organizations, and some variation of the model can be found in many accounting, auditing, management and psychology textbooks:

1. Obtain as many available relevant facts about the given dilemma.
2. Identify and verbalize the ethical issues included in the facts.
3. Identify and list all known stakeholders (both internal and external).
4. Identify and list the ethical principles involved.
5. Brainstorm alternatives available as reactions to the dilemma, including the likely consequences of each alternative.
6. Exercise judgment to determine the best course of action among the alternatives.

These steps have been used to help identify the best solution to the dilemma at Amedisys.

### The Best Course of Action

Following the six-step model, there are three relevant facts in the CA vs. CM dilemma:

- IT auditors create ACL scripts to conduct CA.
- Management personnel (auditees) recognize the value of the scripts and want to use scripts for CM of their own activities.

- The expertise of writing and maintaining the scripts resides with the IT auditors.

The ethical issue is that the IT auditors want to add to total corporate value by assisting management with their CM efforts, but also need to maintain independence and objectivity when providing CA.

The primary stakeholders in the dilemma are the internal audit department and management. Other stakeholders include company employees, stockholders, other third parties, and other members of the IT governance and internal audit professions. The primary ethical principles at issue here are independence and objectivity. Three alternative actions have been identified, along with their associated consequences:

1. IT auditors continue to create and maintain scripts to be used by themselves and management. This will result in the loss of auditor independence and objectivity.
2. IT auditors stop sharing their scripts. Doing so forces management either to learn how to create and maintain its own scripts or hire consultants to do the work.
3. Allow management to use scripts developed by the IT auditors as long as all parties understand their own responsibilities and parameters for creating and maintaining scripts once given to an auditee. Scripts developed by IT auditors are to be used by them for the purpose of CA. In turn, scripts, including those in which management participates in development, can be used by auditees for CM with the understanding that they must take total responsibility for learning to use and maintain the scripts for themselves.

### Figure 2—Agreement of Continuous Monitoring Usage of Internal Audit Scripts

Internal audit develops ACL scripts or other continuous audit tools to continuously audit certain processes or controls within the company. As a member of management, you have requested the use of an ACL script or continuous audit tool to monitor a control within your area on a continuous basis. As a member of management, you are responsible for designing controls. Internal audit has developed a method of automating the control to be used on a continuous basis.

Management within the \_\_\_\_\_ department has requested use of the following script(s):

*(scripts listed and described here)*

To gain access to the internal audit script(s) or continuous auditing tool, you must sign this form stating that you understand and agree to the following:

- Scripts developed for continuous auditing may be used for continuous monitoring by management.
- Internal audit will not request modifications to a script.
- Management is responsible for reviewing the contents of the script and testing it to ensure that results are those expected and anticipated.
- Internal audit is not responsible for any misconceptions on behalf of management in reference to the intended results of running a script.
- Management has the ultimate responsibility of evaluating scripts and testing results to determine if scripts meet the needs.

Internal audit will review script procedures with management and walk through initial execution of the script to ensure that an adequate knowledge transfer occurs for management to conduct continuous monitoring.

Scripts used by management must be stored in a directory separate from the storage of internal audit scripts. Access to each directory must be secured adequately. Access to internal audit scripts must be limited to the internal audit department and required domain administrators to maintain the integrity of the audit script (i.e., audit test).

As a member of management, please sign here stating that you agree to the requirements for script usage listed above.

\_\_\_\_\_  
Name

\_\_\_\_\_  
Name

\_\_\_\_\_  
Position Title

\_\_\_\_\_  
Position Title

## Conclusion

Amedisys has chosen the third alternative as the best response to this dilemma. This alternative allows the IT auditors to maintain their independence and objectivity by permitting them to share scripts with management as a residual result from performing their primary function of CA. Auditor independence and objectivity are maintained by having respective management personnel accept ownership, performance and maintenance of the scripts given to them. With the choice of this solution, formal policies and procedures over the development of scripts by IT auditors have been drafted and implemented within Amedisys. These policies and procedures are shown in the CM agreement form provided in **figure 2**.

The CM agreement form must be signed before the auditee takes possession of a script of interest. The policies and procedures documented in the form are most explicit with identifying the activities of CA and CM, as well as what internal audit can and cannot do for the auditee. IT auditors provide the script, review script procedures with the auditee and walk through the initial execution of the script. After this, the auditee is responsible for testing, running, modifying and securing the script. These procedures provide the necessary level of independence and objectivity required by ISACA and the IIA for the IT governance and internal audit professionals who provide CA. The procedures allow auditees to leverage internal audit's expertise while accepting total responsibility for learning and maintaining the scripts received.

Ethical dilemmas are often described as slippery slopes; unseen until one falls and is unable to regain sure footing. One such slope facing IT auditors is how a misunderstanding of the difference between CA and CM can lead to impairment of their independence and objectivity. With sensitivity and awareness for identifying such a dilemma before the slope gets too steep, IT auditors can make certain they have sure footing by taking careful steps when making decisions that provide valued services to their organization and are enhanced by their independence and objectivity.

## Endnotes

- <sup>1</sup> ISACA, Code of Professional Ethics, 2007, [www.isaca.org/ethics](http://www.isaca.org/ethics)
- <sup>2</sup> The Institute of Internal Auditors, Code of Ethics, 2000, [www.theiia.org](http://www.theiia.org)
- <sup>3</sup> Institute of Management Accountants, The Rights and Responsibilities of a Certified Management Accountant, 2006, [www.imanet.org](http://www.imanet.org)
- <sup>4</sup> American Institute of Certified Public Accountants, Code of Professional Conduct, 2006, [www.aicpa.org](http://www.aicpa.org)
- <sup>5</sup> International Federation of Accountants, Code of Ethics for Professional Accountants, 2005, [www.ifac.org](http://www.ifac.org)
- <sup>6</sup> ISACA Standards Board, "Continuous Auditing: Is It a Fantasy or a Reality?," *Information Systems Control Journal*, 2002, vol. 5, p 43-46
- <sup>7</sup> *Ibid*.

### **Jill Joseph Daigle, CISA, CIA, CISSP**

is the internal audit manager at Amedisys Home Health Services. She has 15 years of experience in internal audit, with 10 of those years as an IT auditor, primarily in healthcare organizations. She can be reached at [jdaigle@amedisys.com](mailto:jdaigle@amedisys.com).

### **Ronald J. Daigle, Ph.D., CPA**

is an assistant professor of accounting at Sam Houston State University (Texas, USA). He teaches auditing and accounting information systems and has published articles on the demand for continuous auditing. He can be reached at [daigle@shsu.edu](mailto:daigle@shsu.edu).

### **James C. Lampe, Ph.D., CPA**

is an associate professor in the School of Accountancy at Missouri State University (USA). He teaches ethics and professionalism, auditing, and IT auditing. He has published articles on professional ethics for accountants and auditors and on the demand for continuous auditing. He can be reached at [jlampe@missouristate.edu](mailto:jlampe@missouristate.edu).

## The Auditor's Choice

To expose suspected errors



**WizRule®**  
business rules detector

To reveal similar or identical records



**WizSame®**  
duplicate records discovery

for a live online demonstration visit [www.wizsoft.com](http://www.wizsoft.com)

**WizSoft®**

(516) 393-5841 • [info@wizsoft.com](mailto:info@wizsoft.com)

# ALLIED SEARCH, INC.

Professional and Executive Search  
Nationwide - All States  
[www.alliedsearchinc.com](http://www.alliedsearchinc.com)

**Corporate Address**  
Allied Search, Inc.  
2030 Union Street, # 206  
San Francisco, CA 94123

**Contact Information**  
Tel. 415-921-1971  
Fax. 415-921-5309  
[donmay@alliedsearchinc.com](mailto:donmay@alliedsearchinc.com)

**Mailing Address**  
Allied Search, Inc.  
P.O.Box 472410  
San Francisco, CA 94147

## OPPORTUNITIES NATIONWIDE

**POSITIONS:** IT Audit Positions and other positions that require or prefer IT Audit experience.

**LEVELS:** All levels of responsibility; staff up to Vice President (VP).

**CLIENTS:** Large Companies In All Industries.

**COMPENSATION:** Very attractive salaries and bonuses.

**BENEFITS:** Excellent benefits.

**LOCATIONS:** U.S. cities nationwide; all fifty (50) states.

**RELOCATIONS:** Relocation assistance is available.

**TRAVEL:** Travel varies from company to company (0% to 100%).  
Some companies have international travel.

**EXPERIENCE:** Prior experience with a Big 4 Professional Services Firm is preferred, but not required.

**COST:** Free to applicant candidates; client companies pay our placement fee.

**CONFIDENTIALITY:** Confidentiality is assured.

**APPLICATION:** Send your resume on a "confidential" basis by one of the following:  
Email: [donmay@alliedsearchinc.com](mailto:donmay@alliedsearchinc.com)  
Fax: 415-921-5309 Attn.: Don May  
Mail: ALLIED SEARCH, INC.  
P.O. Box 472410  
San Francisco, CA 94147-2410  
Attn: Donald C. May, Managing Director

**PROCESS:** After your resume is received, the Managing Director will call you on a "confidential" basis to discuss your background, your objectives and our search assignments that match your background and objectives.

**INTERVIEW TIPS:** Before your first interview, we will discuss with you "How to successfully take the interview and get an offer."

**REFERRALS:** Referrals are appreciated.

**INQUIRIES:** If you have any questions, call Don May at 415-921-1971 on a "confidential" basis. If not in, please leave your name, message and phone number, and your call will be returned as soon as possible, on a "confidential" basis.



# Computer-assisted Audit Techniques: Value of Data Mining for Corporate Auditors

*By John Ott, CISA, CPA, Andrew MacLeod, CISA, CIA, FCPA, MACS, PCP,  
and Kevin Mar Fan, CISA, CA*

**A**udit management staff members are constantly challenged to cut time in completing testing. They evaluate automated controls constantly by reviewing system options, edit logs, etc. They ask themselves: Are information technology (IT) auditors getting the most out of the available technology that can enable financial/operational auditors to effectively perform their duties to detect inefficient and ineffective processes including identifying fraud, waste and abuse of company resources? The answer can be at management's fingertips if it uses well-known data mining techniques, which are part of continuous auditing.<sup>1</sup>

The automated tools available today, when compared with 20 years ago, are well beyond sorting techniques. These tools are capable of analyzing terabytes of information and searching for patterns that may not be identified easily by manual means. In addition, over the past five years, numerous articles and large consulting practices have been created to assist companies in understanding their data, so they can make the most use of data mining. The largest selling point to obtain resources for establishing a data mining process is that organizations can increase their profitability by identifying process improvements, detecting fraud and improving risk management. Furthermore, the patterns uncovered using data mining help organizations make better, timelier and more profitable decisions. An ancillary benefit to data mining is to assist in identifying data that can be sold to other organizations for profit, assuming that the information cannot be traced back to a single individual and/or is not in conflict with a law or government regulation.

The tools used for data mining can range from simplistic and inexpensive tools, such as Microsoft Access and Excel, to standard industry tools that can be costly, such as Audit Control Language (ACL) and Interactive Data Extraction and Analysis (IDEA). This article is not focused on the automated tools, but the conceptual process of understanding the importance of extracting and analyzing data to assist the auditor in reporting potential inefficient and ineffective processes, including potential fraud, waste and abuse of corporate resources. In addition, this article provides a limited view of statistical methods used to identify unusual behavior or anomalies indicating a need for follow-up by the auditor.

Data mining may be different from the approach of computer-assisted audit techniques common 20 years ago. Specifically, the fundamental differences may include the following:

- Technologies have advanced significantly, enabling the auditors to automatically extract data on a scheduled basis and analyze this data without the need for audit queries to be embedded in the program source code.

- Audit tools have become more powerful and easier to use.
- As a result of the previous two points, auditors can not only analyze single data sets, but can also cross-match data sets to perform much richer analysis, which was difficult to do previously.

## Definition of Data Mining

Data mining is a technique that provides specific information that can detect weaknesses in controls. Furthermore, an objective of data mining techniques is to uncover patterns indicating a broken process and/or develop predictive patterns in business information. The first objective is for the auditors to know the purpose of each data element, including how collective data patterns play a role in business decision making. Typically, there may be hundreds or thousands of data elements or variations that require a great deal of auditors' time in developing an understanding through a partnership with the business owner.

## Potential Financial Benefits of Using Data Mining Techniques

Depending upon the organization, there are numerous methods that can be used to reduce the cost of external and internal audits. There are significant benefits to all parties impacted by audit.

For example, to reduce external audit fees, the IT internal auditor may use data mining to validate interface software that performs data transfers between systems. The successful comparison of data extraction from each system used in data transfer can validate balancing routines that can occur between systems. Using data mining techniques is especially important when validating data transfers between noncore systems, which are created internally, and an enterprise resource planning (ERP) system (e.g., SAP) used to record financial statement journal entries. In addition, data mining can validate the data transfer between the ERP (e.g., Lawson, Oracle) and a financial statement reporting package (e.g., ESSBASE), which is essential to financial statement integrity.

At the request of management, data mining can be used to validate a known control such as a preventive and detective duplicate payment control within the accounts payable system (disbursement process). If properly established, the use of data mining appears to be limitless.

Finally, the use of data mining can reduce the need for auditors to travel to a work site, thus reducing travel expenses for the company. In addition, time is saved by not requesting business management to supply unnecessary supporting

documentation when the process is efficient and effective based upon the values noted from performing a data mining analysis. There is greater precision when using data mining techniques to evaluate the most critical processes, which will result in a greater return on the auditor's time and expense by the company. Truly, there is no downside, except for the risk of not properly establishing a baseline expectation to measure trends.

Ultimately, the real value of data mining is educating the business process owner on the means and methods of identifying fraud, waste and abuse, so it can be embedded within the organization's management controls. In the end, management must accept responsibility for using these means and methods to control the business environment.

## Rules for Data Extraction

First, the IT audit must ensure that the source of the data is extracted as early as possible in the data creation process. Auditors should understand that there is a risk that data are scrubbed or altered, which could impact the level of integrity (and therefore reliability) required for detailed analysis by the auditor. Specifically, the auditors should typically request that the IT group embed a software algorithm to tap the data from point of origin. While use of a data warehouse is an acceptable practice by business users, the integrity of the data becomes crucial when this information is used to ascertain which process elements need further audit review.

Second, the auditor must fully understand all the data elements. The auditor should consult with business analysis to document each data element, including its significance to the critical success factors of the enterprise.

## Initiating Data Mining Methodology

The methods employed by the IT audit group to initiate a data mining exercise could result in a full-fledged continuous auditing process requiring scheduled hours. Furthermore, data mining may lead to a separate continuous assurance process to oversee management data analysis, which requires additional audit resources that audit management may not be able to fulfill. Therefore, audit management should properly plan and have a reasonable perspective before embarking on a data mining exercise.

As with all projects, adequate controls should be established, including project management and system development life cycle controls. However, development methodology, such as agile software development, can be employed to shorten the time frame for developing the necessary queries for data sorting and analysis.

Audit management should ensure that all auditors utilize data mining to better understand potential risks within the various financial and operational processes.

There are other techniques, such as employing the use of Benford's law, also called the first-digit law. Specifically, Benford's law states that in lists of numbers from many real-life sources of data, the leading digit is one almost one-third of the time, and larger numbers occur as the leading digit with less and less frequency as they grow in magnitude, to the point that nine is the first digit less than one time in 20.<sup>2</sup> For example, Benford's law may be used to detect telephone and electric billing errors.

In addition, there are other methods presented in this article, including direct analysis in search of questionable occurrences of values within the data and a statistical method that may be used to identify variations of predictive values within the data.

## Standard Data Analysis

As noted previously, direct analysis in search of questionable occurrences of values within the data is the most common data analysis method employed in data mining. Specifically, data analysis usually begins by searching the data files for specific occurrences of data indicating potential fraud, waste and abuse. Examples of questionable practices, typically revealed by data mining within a sample of financial transaction processes, include:

- Risk associated with revenue:
  - Sales to customers in the last month before the end of an accounting period with terms more favorable than previous months to make sales targets and receive bonus pay without approval of management
  - Sales with affiliates and related parties
  - Abnormal number of order cancellations by specific salespeople after the end of an accounting period
  - Recording fictitious sales to nonexistent customers and recording phony sales to legitimate customers
  - Billings to customers that do not equate to customer contracts (within the contract management system)
  - Excessive number of credit memo and other credit adjustments to accounts receivable after the end of the account period
  - Unusual entries to the accounts receivable subledger or sales journal
  - Unusual reconciling differences between sales journals and the general ledger
  - Journal entries made directly to the sales or revenue account
- Risk associated with inventory:
  - Unusual, excessive inventory adjustment amounts that appear repetitive from cycle counts
  - Significant changes in gross profit percentages
  - Large increases in inventory balances without corresponding increases in purchases
  - Journal entries made directly to the inventory account and not through the purchases journal
  - Increases in certain types of inventory or in branches or other locations not examined by the auditors
  - Slow inventory turnover compared to the past
- Risk associated with disbursement (accounts payable):
  - Invoices from companies with a P.O. box address and/or no phone number
  - Invoices from companies with the same address and/or phone number as employees
  - Multiple companies with different names with the same address and phone number
  - The amount of each invoice from a vendor falls just below the threshold for review
  - Check presented for payment that the company did not issue (two checks deposited with same check number)

## Data Mining Using Statistical Modeling

Aside from the simplistic analytical review noted previously, there may be a need for a more detailed analysis that requires a statistical understanding of the data to ascertain predictive patterns, especially if there are voluminous amounts of data.

Overall, the auditor will strive to know the following:

- Patterns in the database and which ones are critical
- Likelihood that an event will occur
- What the summary of the database tells the customers

In conjunction with the previous list, the auditor should identify key indicators. In addition, the auditor should research what values impact (drive or are predictors of) other values (predictive value). The IT audit must first ascertain the following key indicators to get a general understanding of the key values (e.g., categories with the greatest impact on the company's critical success factors):

- Max—The maximum value based upon a driver (predictor)
- Min—The minimum value based upon a predictor
- Mean—The average value based upon a predictor
- Mode<sup>3</sup>—The most common value based upon a predictor
- Median—The value based upon a predictor that separates the database into two parts containing an equal number of records
- Variance<sup>4</sup>—The measure of how spread out the values are from the average value

Typically, the next step is to create some form of regression analysis that can be used as a predictor. There is at least one predictor that drives the critical predictive value up or down. For example, direct labor time (predictor value) for a construction project drives the variable overhead cost (predictive value) up or down, since it is associated with management of the direct labor time. Another possible example is that reduction in "inventory on hand" over a sizeable time period may increase cash flow. There are numerous predictors that, when combined with a value, provide a predictive pattern that the auditor can use to evaluate the efficiency and effectiveness of a process or determine if there is potential fraud, waste and abuse of corporate resources. This allows the auditor to compare future actual values to determine if the behavior is consistent, identify anomalies and respond sooner.

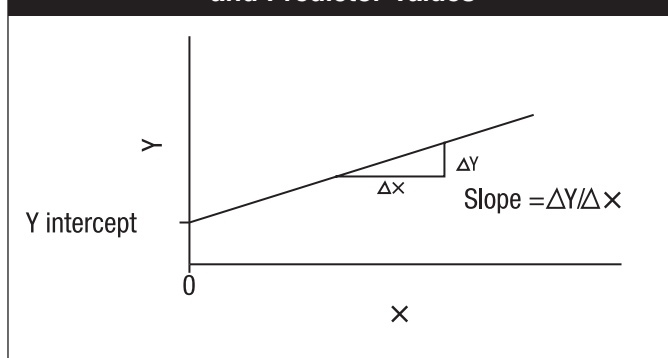
The relationship between the values (predictive and predictor) can be mapped onto a two-dimensional graph. A common method of mapping using linear regression<sup>5</sup> attempts to explain this relationship with a straight line fit to the data:

$$Y = a + bX + e.$$

The "residual"  $e$  is a random variable with a mean of zero. The coefficients  $a$  and  $b$  are determined by the condition that the sum of the square residuals is as small as possible. There is an intuitive assumption that the data are linear and, therefore, it is possible to find the slope and intercept that make a straight line and best fit the data.

As can be seen, this is the simplest form of regression, which seeks to build a predictive model that is a line that maps between each predictor value to a prediction value (see **figure 1**). Of the many possible lines that could be drawn through the data, the one that minimizes the distance between the line and the data points is the one chosen for the predictive model.

**Figure 1—Relationship of Predictive and Predictor Values**



Using a regression model can provide the auditor an easier method of identifying unusual occurrences in the critical values. In addition, adding more predictors (or a variation or multiplication of them) to create the linear equation can produce more complicated lines that take more information into account and, hence, make a better prediction. This is called multiple linear regression, which is beyond the scope of this article, but the auditor should evaluate all aspects when using any model. However, it is up to the auditors to ascertain which values can be used as predictors of critical predictive values. This can be achieved only by understanding the business process and all of the data elements, which may not be a small task. The most important takeaway from this is that the auditor can use a regression model to predict values and, therefore, identify values that indicate potential of an inefficient and/or ineffective process.

## Conclusion

As noted, audit departments can improve their efficiencies greatly by creating or expanding their data mining efforts. In addition, the real value of data mining by auditors is in educating the business owners on using data mining means and methods, including available technologies, to better manage their financial and operational processes. From that point, the hope is that the business owner will take on a continuous monitoring approach. In addition, the auditor must become a strong partner with the business process owners to fully understand the data elements captured within the IT systems that denote an inefficient and ineffective process.

## Endnotes

<sup>1</sup> For the purpose of this article, continuous auditing defines the technologies and processes that allow an ongoing review and analysis of business information on a real-time basis. Continuous monitoring is the process and technology used by management, which could be the result of an audit recommendation, to detect compliance and risk issues associated with an organization's financial and operational environment. Continuous assurance is the audit process that verifies that management's continuous monitoring is operating effectively.

<sup>2</sup> Benford's law states that the leading digit  $d$  ( $d \in \{1, \dots, b-1\}$ ) in base  $b$  ( $b \geq 2$ ) occurs with probability proportional to  $\log_b(d+1) - \log_b d = \log_b((d+1)/d)$ .



1)/ $d$ ). This quantity is exactly the space between  $d$  and  $d + 1$  in a log scale. In base 10, the leading digits have the following distribution in Benford's law, where  $d$  is the leading digit and  $p$  the probability:

$d \rightarrow$	1	2	3	4	5	6	7	8	9
$p \rightarrow$	30.1%	17.6%	12.5%	9.7%	7.9%	6.7%	5.8%	5.1%	4.6%

- <sup>3</sup> The mode values can be utilized via a segmentation method called clustering, which is a method by which like values (records) are grouped together. Clustering may provide the business owner a top-level view of what to expect from similar types of data categories (e.g., customers with purchasing habits). The true value of clustering is the ability to more easily identify changes to critical values that previously behaved similarly to the values in the cluster. This method can be used to identify changes in disbursements and revenue based upon a specific predictor value within the cluster.
- <sup>4</sup> Depending upon the size of the variance, this in itself may be a strong indicator of problems requiring auditor follow-up.
- <sup>5</sup> Statistical prediction is usually synonymous with regression of some form. The line takes a given value for a predictor and maps it to a given value for a prediction. For example, a mutual fund company managing an employee retirement savings account with predicted average yearly retirement savings (in the US) for employees making over US \$100,000 might equal US \$1,000 plus 0.15 multiplied by the employee's annual income.

The goal with predictive modeling is to define values that best minimize the error of not equaling  $Y$  over various values of  $X$ . The most common method to calculate the error is the square of the difference between the predicted and actual

values. Calculated this way, points that are farthest from the line have a great effect on moving the choice of line toward themselves to reduce the error. The values of  $a$  and  $b$  in the regression equation minimize this error, which may be calculated directly from the data.

#### **John Ott, CISA, CPA**

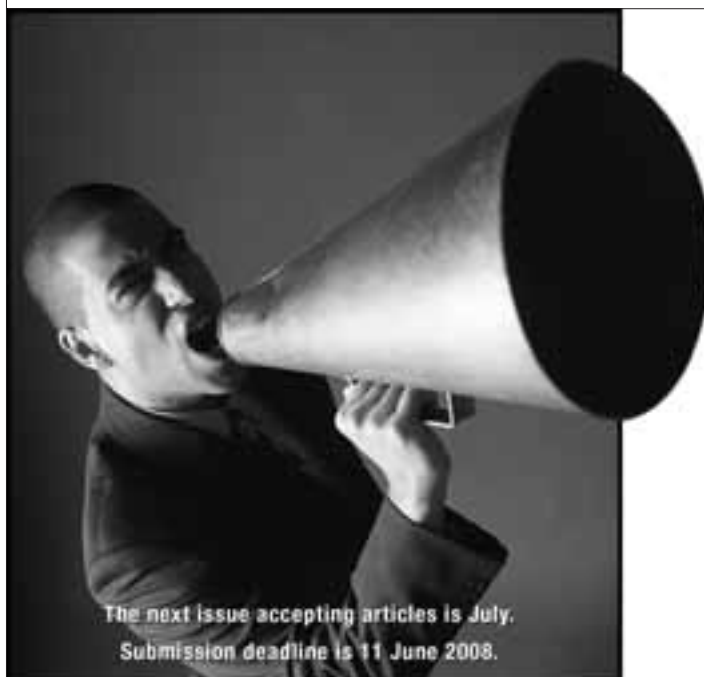
has more than 15 years of experience in several *Fortune* 100 companies. He has specialized in technical IT audits ranging from mainframe and midrange infrastructures to application audits and systems development life cycle reviews. He was a member of the CISA Test Enhancement Committee and is a member of the ISACA Standards Board. He is currently the director of IT audit at AmerisourceBergen, a *Fortune* 29 company.

#### **Andrew MacLeod, CISA, CIA, FCPA, MACS, PCP**

is the chief internal auditor at the Brisbane City Council in Australia, the largest municipal government in the Southern Hemisphere. MacLeod has more than 30 years of experience in information systems and internal audit in Australia and Hong Kong, working with large multinational and major companies in the airline, banking and government sectors. He is a member of the ISACA Standards Board and the Institute of Internal Auditors Professional Issues Committee.

#### **Kevin Mar Fan, CISA, CA**

is a data analysis and continuous assurance manager at the Brisbane City Council, Queensland, Australia. The Brisbane City Council is well progressed in the implementation of continuous assurance. He has more than 14 years of experience in financial and IS audit, working with major multinational companies in Australia, Europe and the US.



The next issue accepting articles is July.  
Submission deadline is 11 June 2008.

## Call for Articles

for *CoBIT® Focus*

*CoBIT® Focus* is the  
CoBIT-based electronic newsletter.

For more information contact  
Jennifer Rajgeorgieva at [publication@isaca.org](mailto:publication@isaca.org)



# Pay Today or Pay Later—Calculating ROI to Justify Information Security and Compliance Budgets

*By Jaspreet Singh, CISA, MCSE, MCSD, BS 7799 LA*

**W**hy do businesses need to calculate return on investment (ROI) for information security? Is the assurance that its network/information technology (IT) infrastructure is secure not good enough? The answer is no, not when information security is viewed as a cost to the business. The only way to get the board of directors to pay any kind of attention is to address ROI.

## Why ROI?

IT departments have traditionally been viewed as cost centers, though they have learned to provide a business case analysis for IT initiatives. Information security departments are trying to figure out how to do the same thing. They cannot sell security initiatives based on fear anymore. Now, they must come up with justifications, complete with the dreaded metrics or hard financial facts.

The business case needs to show specifically how potential costs associated with liability caused by security breaches may be minimized by implementing a sound security infrastructure. This can be accomplished by allowing a third party to do a security audit that provides evidence of security risks.

## How to Capture Loss to Determine ROI

So, how can a business determine how much it will save if it makes a specific investment? There are several methods a business can use, but first it must determine what to measure. The following are five types of loss a business might consider when determining its ROI calculations:

- **Loss of productivity**—For example, if the Internet link of a major software development company goes down, how much time is spent by IT staff repairing damage as opposed to doing other work?
- **Loss of revenue during outages**—A classic case would be the outage of an e-commerce web site. How much revenue might the business lose per minute, per hour or per day in this scenario?
- **Loss of data**—Restoring from a backup can be costly. Plus, the business may not be able to restore all of the data.
- **Repair costs**—The business might need to buy new hardware or use disk-recovery services.
- **Loss of reputation**—There can be negative publicity that can affect the image and reputation of the company.

This is only a partial list; one should think about other areas that could be measured. Should the business take into

account the indirect costs of a breach to the customers, suppliers and stakeholders? How can this be calculated?

## Methodology of Calculating ROI

There are three components to the ROI calculation:

- Identifying actual security risks and translating them into quantifiable business risks
- Identifying how to mitigate the security risks and determining the associated cost
- Calculating the ROI as the percent cost of mitigation divided by the cost of the risk

It is often difficult to quantify expected returns. While the costs can be clearly delineated, most of the time it is more instructive to involve the consideration of “cost of no investment.”

Other common metrics used to measure security risk include:

- **Exposure factor (EF)**—A percentage of loss on an asset if an event occurs. For example, a primary e-commerce web server is compromised and becomes unavailable. The server has been valued at US \$5,000, and the EF has been deemed to be 75 percent.
- **Single loss expectancy (SLE)**—A calculation based on specific monetary value assigned to an event if it occurs. The asset valued at US \$5,000 multiplied by 75 percent equals US \$3,750. This is the cost for a single occurrence of the web site being unavailable.
- **Annual loss expectancy (ALE)**—The expected rate of loss multiplied by the value of that loss. For example, US \$3,750 multiplied by three (expected number of losses in a year) equals US \$11,250.
- **Security savings vs. benefit**—A calculation based on the monetary amount that can be saved by reducing the rate of successful attacks and damage per successful attack

## The Role of Risk Management

It is important to note that, as in any risk assessment scenario, the numbers derived from calculations are not precise and should not be viewed as such. The reason for this is that it is not possible to quantify all possible breaches.

Furthermore, each business must determine the cost of a breach to the organization. For example, the cost of a network compromise to a bank is not the same as the cost to a manufacturing organization. Each organization must look at its business, assess its risk and determine a number that

represents an accurate estimate of these costs per incident. That is, of course, if such costs are tracked.

Then, the organization must determine to what degree a security investment is going to mitigate its risk.

Unfortunately, in the past, ROI rarely has been measured consistently for security projects, if it was measured at all. Many security proposals have been approved based on fears of public disclosure of customer information, regulatory compliance or pressure to keep pace with competitors. That does not mean they have not been necessary, but it makes it difficult to gauge their worth in terms of ROI.

### Benefits of Calculating ROI

Direct benefits of calculating ROI include:

- Reassignment of business and IT employees
- Reduced consulting costs (i.e., as a result of bringing the services in-house)
- Elimination of expenses (e.g., printing, cell phones)
- Reduced development and help desk costs
- Reduced hardware and software maintenance costs

Indirect benefits of calculating ROI include:

- Additional employee productivity
- Reduced hiring (including recruiter fees)
- Reduced training and administrative overhead
- Reduced incidence calls and services
- ALE savings
- Reduced insurance premiums

### The Point of Policy

Once the organization has decided what to measure and which method to use, it should be written into its security policy and assurances should be made to ensure that everyone reports out accordingly. It is vital to maintain consistency over time. A policy establishes stable guidelines. Once something is in a policy, it is harder to change. This should hold true for ROI as much as for other aspects of security. So, to restate, one should:

1. Decide what is going to be measured
2. Decide how it will be measured
3. Write it into the security policy

Return on a security investment can be determined. To do so, one must get the big picture and then drill down to the minutest detail. Once that has been done, one will be close to proving how a security initiative is going to reduce cost, improve productivity and even possibly generate revenue.

### *Jaspreet Singh, CISA, MCSE, MCSA, BS 7799 LA*

is working with Ernst & Young as a manager in its technology and security risk services practice, New Delhi, India. Jaspreet is currently pursuing his Ph.D. in "Developing a Framework for Risk Management for Software Development Companies." He is a regular contributor to leading IT magazines, with topics including legal compliance in India, information security policy and disaster recovery.

According to ITGI's Val IT™ framework, companies that do the following tend to reap significant rewards. Does your organization:

- Continually monitor, evaluate and improve on IT value delivery practices?
- Manage its IT-related initiatives as a portfolio?
- Monitor IT initiatives through their full economic cycle?
- Recognize the different categories of IT-related investments and manage them according to their needs?
- Define and monitor key metrics and respond quickly to changes?
- Assign accountability to appropriate stakeholders to improve benefits derived from IT?

If your organization follows these principles, we'd like to hear from you! Write an article or case study on your organization's experiences managing IT. Please contact Deborah Vohasek at [news@isaca.org](mailto:news@isaca.org).

# Call for Articles

Further detail about these principles can be found in  
*Enterprise Value: Governance of IT Investments, The Val IT Framework*, available from [www.isaca.org/valit](http://www.isaca.org/valit).



# A Business Model for Information Security

By Kent Anderson, CISM

One of the greatest challenges in information security is aligning with business objectives. While practitioners talk about incorporating governance and business requirements, the reality tells a different story. A recent survey showed that 50 percent of North American security professionals' time is spent on reactive and tactical activities such as remediation of operational vulnerabilities.<sup>1</sup> This disconnect between information security operations and strategic business objectives results in pressure to increase security spending while risks, incidents and losses continue escalating to unsustainable levels.

A framework enabling information security professionals to align their activities with their organization's business is needed.

## The Current State of Information Security

Security awareness is at an all-time high. Organizations are spending and hiring information security practitioners in record numbers, and legislation and regulations are proliferating. Despite all of this effort, nearly every statistical measure of performance—from the number of incidents and vulnerabilities to the cost and impact of a breach—demonstrates that the problems are getting worse. More money and technology will not reverse this trend. In what other profession would this level of investment be permitted with such poor return?

The information security profession suffers from several problems that lead to a disconnect between the business and the information security program. Arguably, the greatest is the myopic focus on technology. Many practitioners in the information security field are information technology (IT) engineers and technicians who just “fall into security.” Their training and background is technical, so they overlook the elements that technology depends on: organization, people and process. Effective information security requires a balance among these elements.

This technical focus can isolate the information security function from the other stakeholders in an organization and can create a gap between information security and the business units. Organizational leaders are concerned with other risks, such as physical security, legal, financial and safety, in addition to information and technology. Too often, both sides fail to understand how all of these risks are interrelated.

Effective governance requires organizations to:

- Identify relevant risks
- Determine if security investments are appropriate
- Apply effective and efficient controls
- Align security practices to support and enable the business

Executives and boards of directors are demanding a greater return on their information security investments, and unbalanced security programs cannot deliver the required value.<sup>2</sup> Information security projects frequently fail to meet the business objectives of the organization.

## The Solution: A Business Model for Security

Today's security functions are too often *ad hoc*, reactive and tactically focused.<sup>3</sup> What is needed is a new information security model focused on business, not technology—one that blends technology with the strategic direction and needs of the organization. This can be accomplished by creating an “intentional information security culture” focused on the organization's governance needs. An intentional security culture has several important characteristics:

- **Aligned information security and business objectives**—The model must enable and support business objectives. The information security program should align with the organization from the boardroom to end users, and information security controls should be practical and provide real, measurable risk reduction.
- **A risk-based approach**—Information security controls often are implemented with little or no assessment of the actual risks and threats to an organization, which results in failure to protect valuable assets or wasteful overprotection. Information security practitioners must understand the business—its objectives, operating and regulatory environment, potential threats, risk impacts, operational flexibility, and resilience. Only then can appropriate controls be selected to mitigate risk effectively.
- **Balance between organization, people, process and technology**—Effective risk management requires organizational support, competent people, efficient processes and the selection of appropriate technology. Each element interacts with, impacts and supports the other elements, often in complex ways, so it is crucial to achieve a balance among these elements. If any one element is deficient, information security is diminished.
- **Allowance for the convergence of security strategies**—To maximize return on investment, all security functions (information security, physical security, etc.) should be aligned and support each other. Nonaligned security functions are wasteful and hinder the identification and mitigation of cross-functional risk.
- **Technical and environment neutrality**—The model needs to be independent of any particular technology or technical changes over time. Likewise, the information security model should be applicable across industries, geographies, and regulatory and legal systems.

## The Model's Origin: MSB's Systemic Security Management Framework

The University of Southern California (USC)'s Marshall School of Business (MSB) formed the Institute for Critical Information Infrastructure Protection (ICIIP) to investigate ways to protect information infrastructures. The ICIIP's research led to the development of the Systemic Security Management framework.<sup>4</sup> This framework takes the traditional elements of people, processes and technology, and adds

organizational design and strategy. The Systemic Security Management model recognizes that these elements (referred to as nodes) are interrelated and connected in dynamic and sometimes conflicting or competing ways. The interactions between nodes are called tensions. The critical security elements and their tensions are shown in **figure 1**.

The addition of organization as a key element on the systemic model addresses a significant issue with many information security programs: the disconnect from the other stakeholders in the organization.

As defined by the USC paper, “organization” encompasses the “structures and strategies that enable the enterprise to compete effectively, create competitive advantages, understand its tolerance to risk and adapt governance policies that elevate security to a first priority, a board level issue, pervasive throughout the enterprise.”<sup>5</sup>

**Figure 1—MBS Systemic Security Management Framework**



Source: Kiely, L.; T. Benzel; “Systemic Security Management: A New Conceptual Framework for Understanding the Issues, Inviting Dialogue and Debate, and Identifying Future Research Needs,” Institute for Critical Information Infrastructure Protection (ICIIP), University of Southern California Marshall School of Business, USA, 23 April 2006

From an information security practitioner’s perspective, the interplay and dependencies among these elements—the tensions—create the opportunity to align the information security program with the business by focusing on the issues that too often are overlooked. The tensions are culture, governance, architecture, human factors, enabling and support, and emergence. Emergence “is a dynamic process of patterns occurring over time that seem not to be created by a single entity, person, event or rule...”<sup>6</sup> and represents the complex interactions between people and the processes (both formal and informal) used to perform their job.

These tensions interact with each other and the nodes in complex, dynamic and sometimes competing ways. The role of information security is not to eliminate these tensions, but rather to recognize and understand their effect of risk. Recognizing these tensions creates a more comprehensive information security program by addressing the whole organization. For example, some of the benefits gained when the tensions are considered include:

- Incorporating the needs of different stakeholders
- Recognizing new and unidentified risks and evaluating them cross-functionally
- Linking different information security value chains within the context of the extended enterprise (i.e., manage the loss of perimeter)

- Facilitating the analysis of risks and control implementations on the whole organization

A critical component of this new model is that the technology element is not restricted to a particular vendor, architecture, protocol or standard and, more important, focus is not on the technology, but rather the interaction of the technology with the rest of the organization; therefore, it is technology neutral.

## Next Steps

ISACA’s Security Management Committee (SMC) recognizes the need to unify information security with the business mission of the organization. To this end, the SMC is currently investigating MSB’s Systemic Security Management framework as the basis for a new business model for information security. A critical requirement is to turn the theoretical framework into a working model that can be used by information security practitioners. This requires the careful definition of terms, a better understanding of the tensions and the development of assessment capabilities.

The SMC also recognizes the need for the resulting model to:

- Address the business needs of organizations
- Apply internationally across different cultures and regulatory environments
- Scale from small to large organizations
- Be suitable to all types of organizations—profits, nonprofits, governmental bodies, etc.

ISACA believes the Systemic Security Management model can be developed to meet all of these requirements, allowing information security professionals to align with their organization’s business objectives.

## Endnotes

<sup>1</sup> Deloitte & Touche LLP and Ponemon Institute, “Enterprise@Risk: Insights into the Emerging Privacy and Data Protection Function,” 2007

<sup>2</sup> Anderson, K.E.; “Convergence: A Holistic Approach to Risk Management,” *Network Security*, vol. 2007, iss. 5, May 2007

<sup>3</sup> *Op cit*, Deloitte & Touche

<sup>4</sup> Kiely, L.; T. Benzel; “Systemic Security Management: A New Conceptual Framework for Understanding the Issues, Inviting Dialogue and Debate, and Identifying Future Research Needs,” Institute for Critical Information Infrastructure Protection (ICIIP), University of Southern California Marshall School of Business, USA, 23 April 2006

<sup>5</sup> *Ibid*.

<sup>6</sup> *Ibid*.

## Author’s Note:

The author would like to thank the members of ISACA’s Security Management Committee for their assistance and support in the development of this article.

## Kent Anderson, CISM

is a leading authority on security, with more than 22 years of experience in the field. He serves on ISACA’s Security Management Committee and is the founder and managing director of Network Risk Management LLC.

# Virtual Appliances—The Evolution of a Gold Standard

*By Ronan Kavanagh*

Everybody is talking about virtualization and the amazing potential infrastructural cost and even environmental saving accrued by its deployment. One area of virtualization currently gathering momentum is that of virtual appliances. Where traditional appliances supplanted the office and data center software (server configuration), virtual appliances have taken this to a new level. Where appliances address critical needs not addressed by office servers, they also introduce further complexities and difficulties that are easily resolved by virtual servers. These include ease of evaluation and testing, ease of deployment, streamlined redundancy and backup, and the key benefits of scalability and mobility.

In practical terms, for today's chief information officer (CIO), this offers improved efficiencies in processes, allowing for an emphasis shift from management and control of hardware associated with the solutions, to greater focus on the control of the business requirements.

## The Need for Scalable Architecture

Most organizations today spread their applications across servers based on functional boundaries. Large and small companies use e-mail servers, file servers, web servers and so forth. Over time, the trend has been to dedicate a specific server for each function; this allows for a scalable, highly flexible architecture. As the organization grows, greater demands are placed on the infrastructure, not just from an increase in the number of users, but also in terms of the geographic footprint. Branch offices will require their own servers for certain applications. Fault tolerance also plays a part, driving larger installations toward multiple, duplicated servers, instead of a single monolithic system.

As servers do not generally require user interaction, the trend has been to use vendor-supplied appliances for certain types of applications. An appliance allows for a relatively small footprint and also provides more of a plug-and-play infrastructure over the traditional server application experience. As load increases, new appliances can be brought on-stream and the load distributed evenly. The system administrator can maintain a surplus of similar appliances and install these in the event of failure or increased load. Dividing the application base into component parts and spreading these components across multiple appliances is a tried and tested method of delivering a scalable architecture.

However, industry research shows that the system usage per appliance can be as low as 15 percent of the available processing power.<sup>1</sup> Effectively, the server budget is more than 600 percent higher than necessary. Maintaining a pool of idle

servers on standby in case of increased load or for failure recovery can adversely affect the efficiency even further. Amalgamating applications on each server can go a long way toward resolving the usage issues but at a cost. Running different applications on the same server loses the scalability of the appliance solution and can create security issues.

In addition, maintaining a homogenous environment of appliances is extremely difficult, if not impossible. Complicating this is the need to upgrade different applications at different times. A new appliance can have a different platform configuration, which makes it difficult to migrate users from an older appliance to a new one.

## Virtual Appliances

A virtual appliance is one that subdivides the physical hardware into multiple virtual machines. Each virtual machine provides a self-contained appliance layer to the application. Thus, virtual appliances can be distributed across the set of systems merely by transferring a virtual appliance image, allowing immediacy of deployment and data availability within moments. Load balancing can be achieved among different servers with no requirement to physically move the appliance. The virtual image simply is transferred to the appropriate server.

Any given server can be running a widely disparate range of applications. Therefore, server loading can be controlled tightly by distributing tasks across physical servers. The resources can be shared equitably across the application pool. Memory utilization, disk utilization and, of course, processor utilization can be balanced and controlled more accurately.

By encapsulating each application in its own virtual appliance, the needs of that particular application can be tuned more precisely. Virtualization provides all of the benefits of the traditional appliance with the following additional key benefits:

- Ease of evaluation and testing
- Ease of deployment
- Redundancy and backup
- Scalability and mobility, including improved resource planning and control

## Ease of Evaluation and Testing

Virtualization software's origins come from the area of application testing, mainly allowing the tester to evaluate different applications on a single server. With virtual appliances, these principles still ring through, but when compared to conventional appliance testing, the improved test times, data controls and retention are plain to see.



To evaluate a new appliance, a sample appliance must be shipped, often weeks before the appliance is available for testing. On completion of the evaluation, the sample appliance must then be shipped back to the manufacturer. Even in the event that the appliance is purchased, generally a new appliance must be shipped as the sample appliance is “shop soiled” and unavailable for sale. Further to this, often it is a requirement of evaluation that the appliance be tested within the data center or at a remote geographic location. This adds further difficulties in installing and performing the evaluation, as the tester must arrange for the appliance to be further delivered to the data center and installed.

However, virtual appliances allow the user to load the virtualized image onto an existing server or desktop and begin evaluation and testing immediately. On completing the evaluation, the administrator or evaluator simply can remove the virtual image and the system is restored to its original state.

By encapsulating the server image in a single file, it is possible to duplicate the image and revert to an earlier image as necessary. By using a virtual server, the test team can produce a pristine installation and duplicate that image. For each test, they can then begin the process—starting with a copy of the pristine image—and be confident that there are no vestiges of the previous test.

Extensive testing in a real-life environment can begin almost immediately after the preliminary configuration. At any point during the evaluation, it is trivial to revert to the original installation without the need to ship a new appliance. The evaluation can also be performed on the latest version of software available, as opposed to the version of software that was imaged onto the physical appliance during the manufacturing process.

At the completion of an evaluation, it is often essential to retain the test data or evaluation data for some period of time until decisions have been made by other teams or senior management. In a typical case, this requires that the sample appliance sit idle until such time as it is free to be reinstalled and redeployed.

In the case of virtual appliances, old evaluation and test images can be saved to tape or other backup medium for future analysis or further testing, thus freeing the test system for other tests. Similarly, the test system can be restored easily to a pristine state by the application of a new image, which prevents cross-contamination of tests.

This increased level of control and data access allows for improved analytical decision making by the CIO, rather than having to base “buy” decisions on information or products no longer available for verification.

## Ease of Deployment

Ease of deployment is a key requirement for any organization. The ability to be able to migrate an image onto a new virtual appliance cannot be overstated. Each virtual image contains all the necessary components to deliver the required service or function. The image can be deployed effortlessly to any virtual machine in any location.

In the traditional appliance environment many of the drawbacks associated with the testing are carried through to

the deployment stage. Hardware must be delivered, prestaged and then shipped to its final destination. Frequently, the person performing the initial configuration or prestaging is not the same person performing the physical installation, which can raise several issues. Most notably, changes in physical topography can render the prestaged configuration obsolete. Also, it is often the case that the configuration must be performed by a specialist. This means that the physical appliance must be installed at the data center prior to the arrival of the specialist.

By way of contrast, utilizing a virtual server application decouples the server deployment and the deployment of one or more virtual appliances. Building and configuring a separate operating system to deploy the product simply is not required. Therefore, data are secure from malware and other such security threats without hesitation. Virtual appliances can be deployed as soon as they become available. Any specialist knowledge can be applied without the need for scheduling. No issues arise from the physical topology, as little or no change is required.

Being able to deploy a new e-mail security gateway simply by attaching the image to the virtual server application allows an organization to bring up the new security system in a matter of minutes instead of hours or even days. As the virtual appliance operating system is managed by the vendor, this negates the requirement for knowledge of multiple operating systems, thus reducing potential security risks, increasing operational efficiencies and removing a large management overhead into the future.

Virtual appliances are controlled and managed via a single platform, the virtualization software. This provides the additional benefit of a single source of audit information rather than the requirement for multiple-server auditing.

## Redundancy and Backup

It is essential in this day and age that organizations, regardless of size, plan for the possibility of disaster. In fact, it could be considered to be more important for smaller organizations, as large companies have significant resources to specifically deal with redundancy, backup and disaster

recovery. In contrast, smaller companies frequently struggle with maintaining offsite backups for the different appliances deployed. Often, each appliance has its own backup schema, which make automation difficult, if not impossible, and require specialist

knowledge by the person tasked with maintaining backups.

A virtual appliance encapsulates all of the required bits for that server in an image file. It is possible to back up the image file on a nightly basis and to automatically copy the image to an offsite facility using the Internet. As the appliances within the organization become virtual, the mechanism for backing them up becomes standard across all appliances. Eventually, an automated task can perform the backup operation for all of the virtual images. This standardization reduces the management complexity and associated audit process.

In the event of a disaster, the image can be redeployed and the only losses to the organization are the data produced since the last backup. By using virtual server images, the

---

*The test system can be  
restored easily to a  
pristine state.*

---

organization can even redeploy its server pool without needing to replace much hardware. Several companies offer a “hot standby” site that can be tailored to virtual server images, allowing staff to resume work almost immediately.

It is also far easier to manage duplicated server applications using virtual servers. If the organization has five or six server applications, such as an e-mail security gateway, web content filter gateway, customer relationship management (CRM) application and so on, replicating these applications can require five or six additional appliances. Using virtual servers, it is possible to replicate all of the server applications with as few as two physical systems.

Building redundancy into a physical appliance solution has many challenges, largely based on the expense associated with the supply and logistics of vendor-supplied units to potentially disparate locations. It involves complex planning and difficult execution. The use of virtual appliances removes many layers from the process. Due to the flexibility of virtual appliances, new approaches can be adopted to reduce overall costs and improve success.

For example, in a multibranch organization, each branch office requires its own e-mail security server, domain server and so on. Generally, distributing the applications to each of the remote offices requires a different appliance for each application. Virtualization is almost essential in this case, as it allows each branch office to deploy a single hardware system with multiple virtual appliances instead of multiple physical appliances. Thus, the head office administrator can distribute the virtual appliance suite based on each appliance and on demand, rather than on geography. New servers can be deployed and load-balanced with virtual machines at each outpost, purely centered on real-time requirements.

Backing up a virtual image is relatively straightforward in comparison to backing up a live system disk. Being able to represent the entire system as a virtual image has many advantages, particularly in terms of nightly backups or in the event of a restoration from archive. Should a given system fail, which is not at all unusual, the backed-up images can be redeployed immediately on another virtual machine

with little or no downtime. Another virtual server can be instantiated quickly with the saved image. By using virtual appliances, the availability of the system can be maintained without the need for expensive, redundant appliances or systems. Once the server has been repaired or replaced, the virtual machines can be migrated off the temporary server with minimum fuss or downtime. For example, in a case where the branch office is in Honolulu, Hawaii, USA, and the head office is in San Francisco, California, USA, and the server in Honolulu breaks down, the administrator in the head office can relocate the virtual appliance images to another server, possibly even in another location such as the Los Angeles office. He/she can also arrange for a local supplier to provide a new server to the offshore office or to repair the existing server. Once the server is again available, the virtual appliance image can be migrated back to the Honolulu office with no downtime and no expensive travel time.

---

*New approaches can be  
adopted to reduce overall  
costs and improve success.*

---

## Scalability and Mobility

Organizations generally grow in size. However, they can also shift laterally with personnel from one department being redeployed to another department. This kind of growth can create considerable scalability headaches for IT management. Demand for a particular server, such as the e-mail security appliance, can grow dramatically overnight. Other influences, such as an increase in e-mail due to promotional activity, or a sharp increase in spam due to certain spamming campaigns, can also increase the load on a given appliance. The ability to be able to increase the physical characteristics of the platform, or migrate an appliance from one server to another larger one, provides a fast and effective mechanism for dealing with demand. The ability to instantiate an additional antispam server can also assist with short-term demand and offers a fast route to load balancing.

Attempting to prebuild this type of architecture using only physical appliances can create considerable space and cost difficulties, as it requires that the organization plan for the largest throughput and build out accordingly. This also leaves no possibility of handling peak demand in a more rational way, for example, by having additional capacity that can be deployed for specific tasks. For example, it may be that a given company has a large web site promotion that is due to come to an end. In addition, the campaign has resulted in a significant increase in e-mail messages received. As the number of “hits” on the web site starts to fall off, spare capacity can be redeployed to deal with the additional volume of inbound e-mail by reconfiguring the virtual appliances or creating additional instances of the e-mail security appliance and removing instances of the web site.

The ability to lift an application from one virtual machine and deploy it on another provides a powerful framework for rolling out services across the organization. As the head count

grows, new virtual machines can be instantiated and the number of virtual machines driving a specific application can be increased to meet demand. Likewise, reduced demand for certain applications can be addressed by removing the image from one or more virtual machines, freeing up these resources for other applications. From a geographic perspective, new applications can be deployed at remote sites simply by copying the virtual image to the server or servers at the remote site.

When a specific server needs to be taken offline for any reason, the virtual images executing on that server can be migrated to a new virtual machine without issues of platform version or operating system version.

Mobility is absolutely essential for the proper operation of an application group. It can be next to impossible to move a running user base from one physical appliance to another without significant downtime. In the case of mail antispam appliances, user configuration must be migrated, along with live mail data and quarantine files, black lists, white lists and other elements of the configuration. For a large group of users, these characteristics are changing in a nondeterministic way and at an alarming frequency. Small and large companies

alike often schedule appliance transitions months in advance. New appliances are deployed for a month or two while the administrator tries to find a window to migrate the user base. For most companies, these windows fall on weekends when demand is low. However, many organizations find it difficult to find quiet periods even on weekends. Again, mail is a good example. Users often check their e-mail on the road, from home and even on vacation. The unavailability of the mail system for even two days across a weekend can be problematic. Removing the mail security appliance from the picture can result in clogged mailboxes in a matter of hours.

Mobility is a difficult problem to solve. Most often, the solution is to duplicate the data sets on the old server and the new server over a period of time. Mailboxes must be migrated in their entirety, including any hidden extras such as personal black lists, personal white lists and filter rules. Sometimes the application provides tools for exporting and importing the data sets, but again this can raise issues unless the new appliance has an identical release of the mail software or at least a mechanism for realigning the data sets between versions.

Being able to encapsulate the entire e-mail antispam and antivirus appliance into a single image makes mobility and scalability a relatively trivial exercise. The image simply is “removed” from the old virtual server and redeployed on the new one. Within minutes, users are accessing their e-mail on the new server using the same password and same features as always.

### **In the Field: A Case Study With Penn State Intercollegiate Athletics**

Pennsylvania State University (Penn State)’s Intercollegiate Athletics department has embraced virtual appliance technology. According to Philip Mansfield, systems administrator at Penn State, “Part of the responsibility of systems administration is to recognize the flaws in your system and proactively offer a solution before significant turmoil begins. While Penn State had some very well-performing systems in place, the functionality of its antispam software was not performing up to par. Penn State works like most education institutions with a focus on best practice results from any software purchases while fitting within a tightly managed budget. Spam problems were blocking the network and causing multiple delays, which affected the e-mail performance for the entire group of coaches, professors, and support staff.”

Penn State utilized existing in-house e-mail security software, which was installed directly onto the e-mail server. With such a close association of e-mail and antispam scanning, whenever a significant issue with spam was encountered, mail functions would come to a grinding halt and data were at significant risk. With more than 300 coaches and staff sending and receiving e-mails within the Intercollegiate Athletics group, important messages were in danger of being lost.

Not wanting to affect the performance of a busy coaching staff with mundane but quite critical e-mail tasks, it was decided to look for a better method to support the group. To supplement the existing antispam software, a front-end gateway Simple Mail Transfer Protocol (SMTP) solution was

chosen. The institution was looking for a solution that would provide greater spam filtration as well as free up the workload of the back-end provider. By deploying a software system that automatically updates engines as standard, Penn State is now protected from malware and spam-centric threats.

Once the virtual appliance software was deployed, Penn State saw immediate results.

According to Mansfield, “Controls are now in place to allow the peace of mind of secure data. Users no longer are required to go through a huge list of e-mails each day to weed through spam messages. Where some personnel were receiving more than 300 messages in quarantine daily, there are now only 10 with a greater than 99 percent accuracy level. Even with a cautious quarantine level in place, daily spam reporting has gone from an average of 1,900 per day to 210 per day—an almost 90 percent increase in spam filtration.”

### **Conclusion**

Appliances have made an important impact on how organizations manage their application pools. They have allowed administrators to migrate from a strategy of one large server in the corner, to multiple servers. Today, in a networked environment, interconnectivity is the essential ingredient. The systems are distributed based on load and geography. Virtual servers bring this type of distributed computing to a new height. The ability to move applications among servers, either those co-located in head office or in the data center, or those distributed throughout the branch offices, has become a key business requirement. Data are maintained in a central location and can migrate to thousands of users knowing that the control is maintained at one secure spot.

With disaster recovery preying on the peaceful sleep of most business executives, the ability to quickly redeploy an application moments after its host server has failed solves many critical business issues. Therefore, the new frontier of application deployment is the virtual server, where the physical hardware no longer sets the pace. Instead, the virtual machine provides a pliable, portable environment for all kinds of applications in varied locations.

### **Endnote**

<sup>1</sup> VMware White Paper, “Making Your Business Disaster Ready with Virtual Infrastructure,” May 2006

#### **Ronan Kavanagh**

is president and chief executive officer for SpamTitan suite of products. Educated at the National University of Ireland (Galway), he joined Copperfasten Technologies in June 2004. Prior to joining Copperfasten, Kavanagh worked with Eurokom, an Internet security services provider, delivering a wide range of solutions to both government and large blue-chip companies in Ireland. During his time with Eurokom, Kavanagh was responsible for the ongoing sales development of Eurokom’s managed e-mail service. Prior to Eurokom, Kavanagh worked with World of Fruit.com, a company set up by the Fyffe’s Group in Dublin to provide an Internet portal for the global fruit industry.



# HELPSOURCE Q&A

**Gan Subramaniam, CISA, CIA, CISSP, SSCP, CCNA, CCSA, BS 7799 LA**  
*is the global IT security lead for a global management consulting, technology services and outsourcing company's global delivery network. Previously, he served as head of IT security group compliance and monitoring at a Big 4 professional services firm. With more than 16 years of experience in IT development, IS audit and information security, Subramaniam's previous work includes heading the information security and risk functions at a top UK-based business process owner (BPO). His previous employers include Ernst & Young, UK, Thomas Cook (India) and Hindustan Petroleum Corp., India. As an international conference speaker, he has chaired and spoken at a number of conferences around the world.*

*We invite you to send your information systems audit, control and security questions to:*

**HelpSource Q&A**  
*bgansub@yahoo.com*

**Fax to: +1.847.253.1443**  
**Or mail to:**  
**Information Systems Control Journal**  
**3701 Algonquin Road, Suite 1010**  
**Rolling Meadows, IL 60008 USA**

**Q** My company is planning to buy a software application with an aim to store and track all the business continuity/disaster recovery-related documentation. As an IT auditor, I have been asked to work with the business continuity management (BCM) team to ensure that the right product is purchased. I wish you could provide us with a list of features that would be ideal in any standard product. My employer is a global entity, with operations across different countries.

**A** The ideal scenario would be software that will do the planning for you, get it rolled out and tested, and, should a disaster occur, make the plan work. I wish we could locate a software to do all that.

That said, here is my wish list of requirements for typical BCM software; please remember, as usual, my list is only indicative and not exhaustive. My suggestion would be to group and categorise the requirements under different domains such as plan preparation, information repository, management reporting and access controls. Now, to the list:

- The plan details should be able to be captured by country/location/business/facility to the smallest granular entity within the organisation. The resulting list should be dynamic.
- Information should be able to be captured and stored in meeting the BCM life cycle requirements and adhering to industry standards and methodologies. The different phases of a typical planning process, such as requirements gathering, risk assessment, business impact analysis and plan development, should be incorporated in the software as modules to carry out the plan development work in a structured way. It should also be possible to customise the plan methodologies to suit the organisational requirements. For example, the risk assessment methodology should be changeable and in line with the local methodology used already.
- The software should be customisable (in terms of number of fields, field names, etc.) and enable the users to use their own terms and abbreviations reflecting native usage. Any reports printed should also encompass these

native terms. The size of the fields must be adjustable by the users. At the same time, the software should permit the removal of certain unwanted fields.

- The effects of customisation should be carried forward in any future updates and not require any rework from the user end.
- Integration with any standard word processing software to customize texts must be possible.
- An integrated report-generating tool that enables the creation of custom defined reports must be available.
- A provision to import data in standard formats from other systems, where appropriate, should exist.
- The ability to insert attachments of different types, namely pictures, network diagrams, floor plans, seating plans, etc., should exist.
- The ability to generate multiple questionnaires with user-friendly answering options, such as drop-down menus, should exist.
- A 'drag and drop' feature should be available to accomplish a number of plan maintenance tasks. For example, users getting transferred from one business unit to another should be moved with ease using this feature.
- The ability to search and replace texts with the plans, both globally and locally, should exist.
- An audit-trail-related requirement should be a domain by itself. All updates to the plan must be traceable to both individuals and time.
- A granular approach in terms of access controls, i.e., ability to read/write/edit/modify, must be set to individual user level or group level and must be auditable. Administrative- and non-administrative-level accesses must be available, so that sundry users cannot customise the software based on their whims.
- The ability to print the plans at multiple levels, such as enterprise and business units, should be possible. The creation of a global/enterprisewide plan including summarised information by country/business unit/location/facility must be accomplished with limited manual intervention and inputs. Similarly, the plans should be viewable by domains, i.e., data centre plans, network plans, business units plans and facilities plans.

- The software must be able to generate plans catering to specific scenarios. This requires clear linkages with the business impact analysis process.
- Integration with messaging systems, such as e-mails and Short Message Service (SMS), should exist. It should be possible to e-mail directly from the BCM software to one or more users, both standard and non-standard messages, with document attachments, as deemed appropriate. In addition, it should also be possible to send bulk SMS to users in the case of an event leading to a potential invocation of a plan.
- Provisions for capturing the test scenarios and test results should exist.
- Provision of standard forms and templates for plan development and maintenance, including post-exercise and post-disruption assessment forms, should exist.

The above are some of the key requirements from a BCM point of view. Of course, in addition to typical technical domain requirements, you may wish to consider standard requirements in terms of software usability, vendor credentials, service support, etc. Examples of such requirements include the following:

- Vendor provides user support on a 24x7 basis, across different geographies.
- Training and knowledge transfer support are provided as part of the initial deal.
- Details of other corporate entities using this software, with possible referral options, are provided.
- Cost of maintenance information, i.e., how the pricing model works for obtaining future releases for fixing bugs and upgrades with better features, is provided
- Proprietary databases should not be used. This can act as a major stumbling block, if not available.
- Newsletters/blogs are published to keep the user community current on industry developments. Some vendors do conduct

annual user community events where the problems faced by the users are discussed to enable enhancements to the application.

- Provisions exist for consulting assistance to develop and implement the plan, in particular, for those geographies/locations where the availability of skilled/trained BCM resources may be scarce.
- Features exist to run queries that allow users to convert the data entry screens into query or search forms, enabling them to easily obtain information.
- A help feature is available; it should be user-friendly, context-sensitive and hypertext-enabled. Hint clouds, message panels and prompt windows must be available.

**Q** I believe that there is a big rush and glamour attached to achieving certifications. Be it the BS 7799 or its reincarnation ISO 27001 or the latest BS 25999, numerous options are available.

Do you really believe in them? If a company achieves ISO 27001:2005 certification, does it mean that all necessary security controls are in place? What is your view?

**A** Very interesting question, indeed. I think I have addressed similar questions before. If someone believes that they have achieved 100 percent security excellence by obtaining certification, I do not agree, unless the security controls implementation process has been genuine and flawless. A standard such as ISO 27001:2005 can render only a structured framework to implement the necessary controls in an appropriate manner. Good security should be achieved more by design and not by accident. The key is that certified companies have put processes in place to manage and contain the impact of such incidents.

Earn **38** CPE credits.

Courses include:

- Fundamentals of IT Auditing
- IT Audit Practices
- Information Security Management
- COBIT: Strategies for Implementing IT Governance

Register online now!

**[www.isaca.org/trainingweek](http://www.isaca.org/trainingweek)**

**9-13 June**  
**Vancouver, British Columbia, Canada**

**23-27 June**  
**Minneapolis, Minnesota, USA**

**22-26 September**  
**Washington DC, USA**

**13-17 October**  
**Anaheim, California, USA**

**3-7 November**  
**Chicago, Illinois, USA**

**8-12 December**  
**New Orleans, Louisiana, USA**

# CPE?Quiz

## Quiz #118

Based on Volume 1, 2008—Dysfunctional Operations in IT

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

Prepared by Kamal Khan, CISA, CISSP, MBCS

### True or False

#### Milligan and Hutcheson Article

1. Up to 4 gigabytes of data (equating to approximately 20,000 boxes of paper) can be stored in a device as small as a pen.
2. The most common risks of using mobile devices include viruses, worms, theft, fraud and spam.
3. To counter the threat of sensitive data theft when using personal information management applications, firewalls should be used to minimize access.
4. Blackjacking allows for hacking into an enterprise system using a BlackBerry.
5. Failure to protect corporate data may thrust businesses into violation of governmental regulations such as Personal Information Protection and Electronic Documents Act.
6. The key elements necessary for mobile device security are different from those used for the last 20 years.

#### Johnstone and Chung Article

7. According to a study, the median financial loss due to occupational fraud association, with 1,134 cases between January 2004 and January 2006, was US \$159,000.
8. The Statement on Auditing Standards (SAS) No. 98 from the American Institute of Certified Public Accountants emphasizes auditors exercising their professional skepticism to identify risks that may result in a material misstatement due to fraud.
9. Typically, occupational frauds fall into one of three major categories, including corruption, in which a person uses his/her influence in a business transaction to obtain an unauthorized benefit.

#### Farao Article

10. Hypertext Transfer Protocol (HTTP) is one of the services used to manage and configure printer devices. Transmission Control Protocol (TCP) services are used for printing and managing print jobs.

11. As strict password policies are often applied to printers and their user IDs, passwords are very difficult to obtain as they are never printed in printer manuals.
12. The JetDirect port allows anyone who can connect to it to gather information about the printer configuration or download documents.

#### Unwala and Dharmadhikari Article

13. A fragmented monitoring approach exposes organizations to newer business risks and control issues.
14. An ideal real-time command center needs to log only critical security-related events.
15. In the authors' opinion, the least preferable implementation option is to allow a vendor to implement a solution that provides a product and a service.

#### Brennan Article

16. Although the concept of continuous auditing has been around since the late 1980s, the urgency of Sarbanes-Oxley has helped to make it a reality.
17. Because of mixed results, Siemens has put on hold plans to expand the use of audit automation tools to other business processes.
18. One of the benefits companies can expect from continuous auditing is that they can reduce the number of key controls they need to maintain, monitor and audit.

#### Micallef Article

19. If a chief risk officer is appointed, he/she should not be held accountable to the board for his/her actions.
20. The underlying premise of enterprise risk management, as defined in the Committee of Sponsoring Organizations of the Treadway Commission (COSO) framework, is that every entity exists to provide value for its stakeholders.



**Information Systems Control Journal**  
**CPE Quiz**  
**Based on Volume 1, 2008—Dysfunctional**  
**Operations in IT**

**Quiz #118 Answer Form**

(Please print or type)

Name \_\_\_\_\_

Address \_\_\_\_\_

\_\_\_\_\_

CISA, CISM or CGEIT# \_\_\_\_\_

**Quiz #118**

**True or False**

**Milligan and  
Hutcheson Article**

1. \_\_\_\_\_

2. \_\_\_\_\_

3. \_\_\_\_\_

4. \_\_\_\_\_

5. \_\_\_\_\_

6. \_\_\_\_\_

**Johnstone and Chung  
Article**

7. \_\_\_\_\_

8. \_\_\_\_\_

9. \_\_\_\_\_

**Farao Article**

10. \_\_\_\_\_

11. \_\_\_\_\_

12. \_\_\_\_\_

**Unwala and  
Dharmadhikari Article**

13. \_\_\_\_\_

14. \_\_\_\_\_

15. \_\_\_\_\_

**Brennan Article**

16. \_\_\_\_\_

17. \_\_\_\_\_

18. \_\_\_\_\_

**Micallef Article**

19. \_\_\_\_\_

20. \_\_\_\_\_

*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](http://www.isaca.org/cpequiz). It is graded online and is available to all interested parties.*

*E-mail, fax or mail your answers. Return your answers and contact information by e-mail to [info@isaca.org](mailto: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 the year's end for CPE credits.*

**A passing score of 75 percent will earn one hour of CISA or CISM continuing professional education credit.**



**SRV Professional  
Publications**

Exam Preparation Materials by S.Rao Vallabhaneni

- CISM - 2007, 1<sup>st</sup> Ed, Practice (1,000 Q&A) and Theory (NEW, effective from 2007 exams)
- CISSP - 2006, 3<sup>rd</sup> Ed, Practice (1,700 Q&A) and Theory (UPDATED)
- CISA - 2006, 5<sup>th</sup> Ed, Practice (1,700 Q&A) and Theory + CD (UPDATED by ExamMatrix)
- CIA - 2005, 3<sup>rd</sup> Ed, Practice (4,013 Q&A) and Theory + CD (UPDATED by Wiley effective from 2004 exams)
- SSCP - 2002, 1<sup>st</sup> Ed, Practice (800 Q&A) and Theory
- SRVware - CISM, CISSP, and SSCP (Web-based Software with Sample Practice Questions)

For ordering, contact SRV Professional Publications,  
869 East Schaumburg Road, Suite 262, Schaumburg, IL  
60194-3654 USA. Phone: 847-894-1508 Fax: 847-330-1260  
[Info@srvbooks.com](mailto:Info@srvbooks.com) • [www.srvbooks.com](http://www.srvbooks.com)  
U.S. ground shipping is free.

***Get  
noticed...***  
**Advertise in the  
Information Systems  
Control Journal!**

For more information,  
contact

*[advertising@isaca.org](mailto:advertising@isaca.org)*

# MEMBERSHIP APPLICATION

Join online and save US \$20.00

[www.isaca.org/join](http://www.isaca.org/join)

Please complete both sides

U.S. Federal I.D. No. 23-7067291

[www.isaca.org](http://www.isaca.org)

[membership@isaca.org](mailto:membership@isaca.org)

☐ MR. ☐ MS. ☐ MRS. ☐ MISS ☐ OTHER \_\_\_\_\_

Date \_\_\_\_\_

Name \_\_\_\_\_  
FIRST MIDDLE LAST/FAMILY

PRINT NAME AS YOU WANT IT TO APPEAR ON MEMBERSHIP CERTIFICATE

Residence address \_\_\_\_\_  
STREET

CITY STATE/PROVINCE/COUNTRY POSTAL CODE/ZIP

Residence phone \_\_\_\_\_ Residence facsimile \_\_\_\_\_  
AREA/COUNTRY CODE AND NUMBER AREA/COUNTRY CODE AND NUMBER

Company name \_\_\_\_\_

Title \_\_\_\_\_

Business address \_\_\_\_\_  
STREET

CITY STATE/PROVINCE/COUNTRY POSTAL CODE/ZIP

Business phone \_\_\_\_\_ Business facsimile \_\_\_\_\_  
AREA/COUNTRY CODE AND NUMBER AREA/COUNTRY CODE AND NUMBER

E-mail \_\_\_\_\_

## Send mail to

- ☐ Home  
☐ Business

## Chapter Affiliation

- ☐ Chapter Number (see reverse) \_\_\_\_\_  
or  
☐ Member at large (no chapter within 50 miles/80 km)

- ☐ I do not want to be included on a mailing list, other than that for Association mailings.

## How did you hear about ISACA?

- 1 ☐ Friend/Coworker 6 ☐ Local Chapter  
2 ☐ Employer 7 ☐ Certification Programs  
3 ☐ Internet Search 8 ☐ Direct Mail  
4 ☐ Information Systems 9 ☐ Educational Event  
Control Journal

**Please note:** Membership in the association requires you to belong to a chapter when you live or work within 50 miles/80 km of a chapter territory. The name of the chapter is indicative of its territory. If you live farther than 50 miles/80 km from a chapter territory, select member at large. Chapter selection is subject to verification by ISACA International. Cities listed in parentheses are a reference to where the majority of chapter meetings are held. Please contact your local chapter at [www.isaca.org/chapters](http://www.isaca.org/chapters) for other meeting locations.

## Current field of employment (check one)

- 1 ☐ Financial/Banking  
2 ☐ Insurance  
3 ☐ Public Accounting  
4 ☐ Transportation  
5 ☐ Aerospace  
6 ☐ Retail/Wholesale/Distribution  
7 ☐ Government/Military—National/State/Local  
8 ☐ Technology Services/Consulting  
9 ☐ Manufacturing/Engineering  
10 ☐ Telecommunications/  
Communications  
11 ☐ Mining/Construction/Petroleum/  
Agriculture  
12 ☐ Utilities  
13 ☐ Legal/Law/Real Estate  
14 ☐ Health Care/Medical  
15 ☐ Pharmaceutical  
16 ☐ Advertising/Marketing/Media  
17 ☐ Education/Student  
99 ☐ Other \_\_\_\_\_

## Level of education achieved (indicate degree achieved, or number of years of university education if degree not obtained)

- 1 ☐ One year or less 7 ☐ AS  
2 ☐ Two years 8 ☐ BS/BA  
3 ☐ Three years 9 ☐ MS/MBA/Masters  
4 ☐ Four years 10 ☐ PhD  
5 ☐ Five years 99 ☐ Other \_\_\_\_\_  
6 ☐ Six years or more

## Certifications obtained (other than CISA, CISM, CGEIT)

- 1 ☐ CPA 5 ☐ CPP  
2 ☐ CA 6 ☐ GIAC  
3 ☐ CIA 7 ☐ CFE  
4 ☐ CISSP 99 ☐ Other \_\_\_\_\_

## Work experience

(check the number of years of information systems related work experience)

- 1 ☐ No experience 4 ☐ 8-9 years  
2 ☐ 1-3 years 5 ☐ 10-13 years  
3 ☐ 4-7 years 6 ☐ 14 years or more

## Current professional activity (If not your title, please select the BEST match)

- 1 ☐ CEO, President, Owner, General/Executive Manager  
2 ☐ CAE, General Auditor, Partner, Audit Head/VP/EVP  
3 ☐ CISO/CSO, Security Executive/VP/EVP  
4 ☐ CIO/CTO, Info Systems/Technology Executive/VP/EVP  
5 ☐ CFO, Controller, Treasurer, Finance Executive/VP/EVP  
6 ☐ Chief Compliance/Risk/Privacy Officer, VP/EVP  
7 ☐ IS/IT Audit Director/Manager/Consultant  
8 ☐ Security Director/Manager/Consultant  
9 ☐ IS/IT Director/Manager/Consultant  
10 ☐ Compliance/Risk/Privacy Director/Manager/Consultant  
11 ☐ IS/IT Senior Auditor (External/Internal)  
12 ☐ IS/IT Auditor (External/Internal Staff)  
13 ☐ Non-IS/IT Auditor (External/Internal)  
14 ☐ Security Staff  
15 ☐ IS/IT Staff  
16 ☐ Professor/Teacher  
17 ☐ Student  
99 ☐ Other \_\_\_\_\_

Date of Birth \_\_\_\_\_  
MONTH/DAY/YEAR

## Payment due

- Association dues † \$ 130.00 (US)  
• Chapter dues (see reverse) \$ \_\_\_\_\_ (US)  
• New member processing fee \$ 30.00 (US)\*  
PLEASE PAY THIS TOTAL \$ \_\_\_\_\_ (US)

† For student membership information please visit [www.isaca.org/student](http://www.isaca.org/student)

\* Membership dues consist of Association dues, chapter dues and new member processing fee. Join online and save US \$20.00.

Membership dues are nonrefundable and nontransferable.

## Method of payment

- ☐ Check payable in US dollars, drawn on US bank  
☐ Send invoice (Applications cannot be processed until dues payment is received.)  
☐ MasterCard ☐ VISA ☐ American Express ☐ Diners Club

All payments by credit card will be processed in US dollars

ACCT # \_\_\_\_\_

Print name of cardholder \_\_\_\_\_

Expiration date \_\_\_\_\_  
MONTH/YEAR

Signature \_\_\_\_\_

Cardholder billing address if different than address provided above:

By applying for membership in ISACA, members agree to hold the association and its chapters, and the IT Governance Institute, and their respective officers, directors, members, trustees, employees and agents, harmless for all acts or failures to act while carrying out the purposes of the association and the institute as set forth in their respective bylaws, and they certify that they will abide by the association's Code of Professional Ethics ([www.isaca.org/ethics](http://www.isaca.org/ethics)).

Full payment entitles new members to membership from the date payment is processed by International Headquarters through 31 December 2008. No rebate of dues is available upon early resignation of membership.

Contributions, dues or gifts to ISACA are not tax deductible as charitable contributions in the United States. However, they may be tax deductible as ordinary and necessary business expenses.

## Make checks payable to:

ISACA

## Mail your application and check to:

ISACA  
1055 Paysphere Circle  
Chicago, IL 60674 USA  
Phone: +1.847.253.1545  
Fax: +1.847.253.1443

The dues amounts on this application are valid 7 August 2007 through 31 May 2008.

US dollar amounts listed below are for local chapter dues. While correct at the time of printing, chapter dues are subject to change without notice. Please include the appropriate chapter dues amount with your remittance.

For current chapter dues, or if the amount is not listed below, please visit the web site, [www.isaca.org/chapdues](http://www.isaca.org/chapdues), or contact your local chapter at [www.isaca.org/chapters](http://www.isaca.org/chapters).

Chapter Name	Chapter Number	Dues	Chapter Name	Chapter Number	Dues	Chapter Name	Chapter Number	Dues	Chapter Name	Chapter Number	Dues
<b>ASIA</b>			Ireland	156	\$40	<b>Northeastern United States</b>			Las Vegas, NV	187	\$35
Hong Kong	64	\$45	Tel-Aviv, Israel	40	\$50	Greater Hartford, CT	28	\$40	Willamette Valley, OR	50	\$30
Bangalore, India	138	\$15	Milan, Italy	43	\$53	Central Maryland	24	\$25	(Portland)		
Cochin, India	176	\$15	Rome, Italy	178	\$26	(Baltimore)			Utah (Salt Lake City)	04	\$30
Coimbatore, India	155	\$10	Kenya	158	\$40	New England	18	\$30	Mt. Rainier, WA (Olympia)	129	\$20
Hyderabad, India	164	\$20	Latvia	139	\$20	New Jersey	30	\$40	Puget Sound, WA (Seattle)	35	\$25
Kolkata, India	165	\$20	Lithuania	180	\$40	Central New York	29	\$15			
Chennai, India	99	\$10	Luxembourg	198	\$85	(Syracuse)			<b>OCEANIA</b>		
Mumbai, India	145	\$21	Malta	186	\$25	Hudson Valley, NY	120	\$0	Adelaide, Australia	68	\$0
New Delhi, India	140	\$15	Netherlands	97	\$50	(Albany)			Brisbane, Australia	44	\$16
Pune, India	159	\$17	Abuja, Nigeria	185	\$40	New York Metropolitan	10	\$50	Canberra, Australia	92	\$15
Indonesia	123	\$45	Lagos, Nigeria	149	\$20	Western New York	46	\$30	Melbourne, Australia	47	\$15
Nagoya, Japan	118	\$60	Norway	74	\$55	(Buffalo)			Perth, Australia	63	\$10
Osaka, Japan	103	\$85	Warsaw, Poland	151	\$30	Harrisburg, PA	45	\$25	Sydney, Australia	17	\$30
Tokyo, Japan	89	\$80	Moscow, Russia	167	\$10	Philadelphia, PA	06	\$40	Auckland, New Zealand	84	\$40
Korea	107	\$40	Romania	172	\$50	Pittsburgh, PA	13	\$20	Wellington, New Zealand	73	\$28
Lebanon	181	\$35	Slovenia	137	\$50	Rhode Island	197	\$25	Papua New Guinea	152	\$10
Macao	190	\$0	Slovak Republic	160	\$65	National Capital Area, DC	05	\$40			
Malaysia	93	\$10	South Africa	130	\$35						
Muscat, Oman	168	\$40	Barcelona, Spain	171	\$110	<b>Southeastern United States</b>					
Karachi, Pakistan	148	\$20	Madrid, Spain	183	\$85	North Alabama (Birmingham)	65	\$30	<b>To receive your copy of the Information Systems Control Journal, please complete the following sub- scriber information:</b>  <b>Size of ENTIRE organization</b> ① <input type="checkbox"/> Fewer than 50 employees ② <input type="checkbox"/> 50 – 149 employees ③ <input type="checkbox"/> 150 – 499 employees ④ <input type="checkbox"/> 500 – 1,499 employees ⑤ <input type="checkbox"/> 1,500 – 4,999 employees ⑥ <input type="checkbox"/> 5,000 – 9,999 employees ⑦ <input type="checkbox"/> 10,000 – 14,999 employees ⑧ <input type="checkbox"/> 15,000 or more employees  <b>Size of IS/IT audit staff (local office)</b> ① <input type="checkbox"/> 0 individuals ② <input type="checkbox"/> 1 individual ③ <input type="checkbox"/> 2-5 individuals ④ <input type="checkbox"/> 6-10 individuals ⑤ <input type="checkbox"/> 11-25 individuals ⑥ <input type="checkbox"/> More than 25 individuals  <b>Size of information security staff (local office)</b> ① <input type="checkbox"/> 0 individuals ② <input type="checkbox"/> 1 individual ③ <input type="checkbox"/> 2-5 individuals ④ <input type="checkbox"/> 6-10 individuals ⑤ <input type="checkbox"/> 11-25 individuals ⑥ <input type="checkbox"/> More than 25 individuals  <b>Your level of purchasing authority</b> ① <input type="checkbox"/> Recommend products/services ② <input type="checkbox"/> Approve purchase ③ <input type="checkbox"/> Recommend and approve purchase		
Lahore, Pakistan	196	\$30	Valencia, Spain	182	\$75	Jacksonville, FL	58	\$30			
Manila, Philippines	136	\$20	Sweden	88	\$45	Central Florida (Orlando)	67	\$35			
Jeddah, Saudi Arabia	163	\$70	Switzerland	116	\$45	South Florida	33	\$40			
Riyadh, Saudi Arabia	154	\$0	Tanzania	174	\$50	West Florida (Tampa)	41	\$35			
Singapore	70	\$10	London, UK	60	\$25	Atlanta, GA	39	\$40			
Sri Lanka	141	\$15	Central UK	132	\$55	Charlotte, NC	51	\$35			
Taiwan	142	\$50	Northern England, UK	111	\$75	Research Triangle	59	\$25			
Bangkok, Thailand	109	\$10	Scotland, UK	175	\$60	(Raleigh, NC)					
UAE	150	\$10				South Carolina Midlands	54	\$30			
<b>CENTRAL/SOUTH AMERICA</b>			<b>NORTH AMERICA</b>			(Columbia, SC)					
Buenos Aires, Argentina	124	*	<b>Canada</b>			Memphis, TN	48	\$45			
Mendoza, Argentina	144	*	Calgary, AB	121	\$25	Middle Tennessee	102	\$45			
LaPaz, Bolivia	173	\$25	Edmonton, AB	131	\$25	(Nashville)					
São Paulo, Brazil	166	\$20	Vancouver, BC	25	\$20	Virginia	22	\$30			
Santiago, Chile	135	\$40	Victoria, BC	100	\$0				<b>Southwestern United States</b>		
Bogotá, Colombia	126	\$25	Winnipeg, MB	72	\$20	Central Arkansas	82	\$60			
San José, Costa Rica	31	\$33	Nova Scotia	105	\$0	(Little Rock)					
Quito, Ecuador	179	\$15	Ottawa Valley, ON	32	\$10	Denver, CO	16	\$40			
Mérida, Yucatán, México	101	\$50	Toronto, ON	21	\$25	Baton Rouge, LA	85	\$25			
Mexico City, México	14	\$65	Montreal, PQ	36	\$25	Greater New Orleans, LA	61	\$25			
Monterrey, México	80	\$50	Quebec City, PQ	91	\$45	Greater Kansas City, MO	87	\$0			
Panamá	94	\$30				St. Louis, MO	11	\$25			
Asunción, Paraguay	184	\$40	<b>Islands</b>			New Mexico (Albuquerque)	83	\$25			
Lima, Perú	146	\$15	Bermuda	147	\$0	Central Oklahoma (OK City)	49	\$30			
Puerto Rico	86	\$40	Trinidad & Tobago	106	\$25	Tulsa, OK	34	\$25			
Montevideo, Uruguay	133	*				Austin, TX	20	\$25			
Venezuela	113	\$20	<b>Midwestern United States</b>			Greater Houston Area, TX	09	\$40			
<b>EUROPE/AFRICA</b>			Chicago, IL	02	\$50	North Texas (Dallas)	12	\$30			
Austria	157	\$45	Illini (Springfield, IL)	77	\$30	San Antonio/So. Texas	81	\$25			
Belguim	143	\$60	Central Indiana	56	\$30				<b>Western United States</b>		
Sofia, Bulgaria	189	\$40	(Indianapolis)			Anchorage, AK	177	\$20			
Croatia	170	\$50	Michiana (South Bend, IN)	127	\$0	Phoenix, AZ	53	\$30			
Czech Republic	153	\$110	Iowa (Des Moines)	110	\$25	Los Angeles, CA	01	\$25			
Denmark	96	\$50	Kentuckiana (Louisville, KY)	37	\$35	Orange County, CA	79	\$30			
Estonia	162	\$20	Detroit, MI	08	\$40	(Anaheim)					
Finland	115	\$15	Western Michigan	38	\$25	Sacramento, CA	76	\$25			
France (Paris)	75	\$140	Minnesota	07	\$35	San Francisco, CA	15	\$45			
Germany	104	\$80	Omaha, NE	23	\$30	San Diego, CA	19	\$40			
Athens, Greece	134	\$30	Central Ohio (Columbus)	27	\$25	Silicon Valley, CA	62	\$30			
Budapest, Hungary	125	\$65	Greater Cincinnati, OH	03	\$30	(Sunnyvale)					
			Northeast Ohio (Cleveland)	26	\$30	Hawaii (Honolulu)	71	\$40			
			Northwest Ohio	188	\$25	Boise, ID	42	\$40			
			Kettle Moraine, WI	57	\$35						
			(Milwaukee)								
			Quad Cities	169	\$25						

\*Call chapter for information

# Prepare for the 2008 CISA Exams

## ORDER NOW—2008 Certified Information Systems Auditor (CISA) Review Materials for Exam Preparation and Professional Development

Passing the CISA exam can be achieved through 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 (see [www.isaca.org/cisaexam](http://www.isaca.org/cisaexam) for more details).

### CISA Review Manual 2008

ISACA

The *CISA® Review Manual 2008* has been completely revised and updated with new content to reflect changing industry principles and practices, and is organized according to the current CISA job practice areas. The manual features detailed descriptions of the tasks performed by IS auditors and the knowledge required to plan, manage and perform IS audits. The new edition also features new case studies to assist a candidate's understanding of current practices. Also included are definitions of terms most commonly found on the exam, practice questions similar in content to what has previously appeared on the exam and references to additional study materials on specific topics. 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 2008 edition has been developed and is organized to help prepare the CISA candidate in studying the following job practice areas:

- The 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-8** English Edition  
**CRM-8I** Italian Edition  
**CRM-8J** Japanese Edition  
**CRM-8S** Spanish Edition

### CISA Review Questions, Answers & Explanations Manual 2008

ISACA

The *CISA® Review Questions, Answers & Explanations Manual 2008* consists of 600 multiple-choice study questions that have previously appeared in the *CISA® Review Questions, Answers & Explanations Manual 2006* and the *2007 Supplement*. 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 to provide further clarity or explanation of the suggested correct answer. These questions are not actual exam items, but are intended to provide the CISA candidate 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 2008*.

To assist users in maximizing their study efforts, questions are presented in the following two ways:

- Sorted by job practice area
- Scrambled as a sample 200-question exam

**QAE-8** English Edition  
**QAE-8I** Italian Edition  
**QAE-8J** Japanese Edition  
**QAE-8S** Spanish Edition

### CISA Review Questions, Answers & Explanations Manual 2008 Supplement

ISACA

Developed each year, the *CISA® Review Questions, Answers & Explanations Manual 2008 Supplement* is recommended for use when preparing for the 2008 CISA exam. This edition consists of 100 new sample questions, answers and explanations based on the current CISA job practice areas, using a similar process for item development as is used to develop actual exam items. The questions are intended to provide the CISA candidate 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-8ES** English Edition  
**QAE-8FS** French Edition  
**QAE-8IS** Italian Edition  
**QAE-8JS** Japanese Edition  
**QAE-8SS** Spanish Edition

### CISA Practice Question Database v8

ISACA

The *CISA® Practice Question Database v8* combines the *CISA Review Questions, Answers & Explanations Manual 2008* with the *CISA Review Questions, Answers & Explanations Manual 2008 Supplement* into one comprehensive 700-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 the user's previous scoring history, allowing CISA candidates to easily and quickly identify their strengths and weaknesses, and focus their study efforts accordingly. Other features allow the user to select sample exams by specific job practice areas, view questions that were previously answered incorrectly and vary the length of their study sessions. Also included are *Information Systems Control Journal* articles referenced in the *CISA Review Manual 2008*. The database is available in CD-ROM format or as a web site download.

PLEASE NOTE the following system requirements:

- Intel Pentium 3 or higher (Pentium 4 recommended)
- Windows 98SE or higher
- 256 MB RAM (512 MB recommended)
- Hard drive with 225 MB of available space
- CD-ROM drive
- Display with recommended resolution of 1024 x 768

The CISA Practice Question Database v8 is licensed for installation on one computer only for personal, noncommercial use.

**CDB-8** English Edition—CD-ROM  
**CDB-8W** English Edition—Web site download  
**CDB-8S** Spanish Edition—CD-ROM  
**CDB-8SW** Spanish Edition—Web site download

**To order CISA® review material for the June or December 2008 exam, see the order form on page S-8 in this *Journal* or visit [www.isaca.org/cisabooks](http://www.isaca.org/cisabooks).**



## Advertisers/Web Sites

ACL	<a href="http://www.acl.com/red">www.acl.com/red</a>	3
Allied Search*	<a href="http://www.alliedsearchinc.com">www.alliedsearchinc.com</a>	44
Caseware Idea Inc.	<a href="http://www.caseware-idea.com/smartanalyzer">www.caseware-idea.com/smartanalyzer</a>	4
CCH Teammate	<a href="http://www.CCHGroup.com/ISJ">www.CCHGroup.com/ISJ</a>	Inside Back Cover
Citizens Bank*	<a href="http://www.citizensbank.com/employment">www.citizensbank.com/employment</a>	15
Cyber-Ark	<a href="http://www.cyber-ark.com/ISACA108">www.cyber-ark.com/ISACA108</a>	8
ExamMatrix	<a href="http://www.ExamMatrix.com/ISJ">www.ExamMatrix.com/ISJ</a>	15
Favored Solutions	<a href="http://www.favoredsolutions.net">www.favoredsolutions.net</a>	10
KBA	<a href="http://www.kbagroupllp.com">www.kbagroupllp.com</a>	30
Lander International LLC*	<a href="http://www.landerint.com">www.landerint.com</a>	22
Market Central	<a href="http://www.securswitch.com">www.securswitch.com</a>	16
Paisley Consulting	<a href="http://www.paisley.com">www.paisley.com</a>	1
Prevelant Networks	<a href="http://www.prevelant.net/easycompliance.com">www.prevelant.net/easycompliance.com</a>	Inside Front Cover
SRV Professional Publications	<a href="http://www.srvbooks.com">www.srvbooks.com</a>	60
Veridion	<a href="http://www.veridion.net">www.veridion.net</a>	23
WizSoft	<a href="http://www.wizsoft.com">www.wizsoft.com</a>	43

\* Position openings/recruitment listings

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

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

© 2008 ISACA. All rights reserved.

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

#### Subscription Rates:

US: one year (6 issues) \$75.00

All international orders: one year (6 issues)

\$90.00. Remittance must be made in US funds.

ISSN 1526-7407

## Leaders and Supporters

### Editor

Jane Seago

### Senior Editorial Manager

Jennifer Hajigeorgiou  
[publication@isaca.org](mailto:publication@isaca.org)

### Media Relations

Deborah Vohasek  
Kristen Kessinger  
Suzanne Kelly  
[news@isaca.org](mailto:news@isaca.org)

### Contributing Editors

Sally Chan, CMA, ACIS, PAdmin  
Kamal Khan, CISA, CISSP, MBCS  
A Rafeq, CISA, CIA, CQA, CFE, FCA  
Steven J. Ross, CISA, CBCP, CISSP  
Tommie Singleton, Ph.D., CISA,  
CMA, CPA, CITP  
B. Ganapathi Subramaniam, CISA, CIA,  
CISSP, SSCP, CCNA, CCSA, BS 7799 LA

### Advertising

Mohanna & Associates  
[advertising@isaca.org](mailto:advertising@isaca.org)

### Editorial Committee

Chair, Rupert Dodds, CISA, CISM, FCA  
Christopher Budd, CISA, CISM, CISSP, ISMP  
Christos Dimitriatis, Ph.D., CISA, CISM  
Ken Doughty, CISA, CBCP  
Urs Gattiker, Ph.D.  
Francisco Igual, CISA  
Alan Lord, CISA, CPA  
Juan Macias  
David Earl Mills, CISA, MCSE  
Esteban Miyashiro, CISA  
Pak-Lok Poon, Ph.D., CISA, CSQA, MIEEE  
B. Ganapathi Subramaniam, CISA, CIA,  
CISSP, SSCP, CCNA, CCSA, BS 7799 LA  
Carlos Villamizar Rodriguez, CISA

### ISACA Board of Directors (2007-2008):

#### International President

Lynn Lawton, CISA, FBCS CITP, FCA, FIIA, PIIA

#### Vice President

Georges Ataya, CISA, CISM, CISSP

#### Vice President

Avinash W. Kadam, CISA, CISM, CBCP, CISSP

#### Vice President

Howard Nicholson, CISA

#### Vice President

Jose Angel Peña Ibarra

#### Vice President

Robert E. Stroud

#### Vice President

Kenneth L. Vander Wal, CISA, CPA

#### Vice President

Frank K.M. Yam, CISA, FHKIoD, FHKCS, CIA, CCP,  
CFE, CFSA, FFA

#### Past International President, 2003-2005

Marios Damianides, CISA, CISM, CA, CPA

#### Past International President, 2007-2008

Everett C. Johnson Jr., CPA

#### Director

Emil G. D'Angelo, CISA, CISM

#### Director

Greg Grocholski, CISA

#### Chief Executive Officer

Susan M. Caldwell