

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.

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.



IDEA is a registered trademark of CaseWare IDEA Inc.

IDEA significantly improves your ability to detect fraud.

Information Systems
Control Journal becomes
ISACA Journal with volume 1, 2009.
Look for the same industry-leading
topics in a new, updated format.

Information Systems Control JOURNAL

The Magazine for IT Governance Professionals

VOLUME 6, 2008

Columns

5
Guest Editorial: You Can't
Outsource Control
By Edge Zarrella, CISA, CA

9
IS Security Matters: Certification and
the Disappearing Perimeter
By Steven J. Ross, CISA, CBCP, CISSP

12
IT Audit Basics: What Every IT Auditor
Should Know About Auditing Virtual
Machine Technology
Tommie W. Singleton, Ph.D., CISA,
CITP, CMA, CPA

18
IT Value: Practical Guidance on
Establishing the Val IT Value
Governance Process
By Sarah Harries and Peter Harrison,
FCPA

20
Five Questions With...
Antonio F. Pecora, CISA, CISM, CGEIT,
CRP, CFS, CPM, ISSPCS

22
IT Governance: Taking
Governance Forward
By Patrick Stachtchenko, CISA, CA

Features

16
Book Review: Phishing and
Countermeasures: Understanding the
Increasing Problem of Identity Theft
Reviewed by Vishnu Kanhere, Ph.D.,
CISA, CISM, AICWA, CFE, FCA

17
Book Review: IT Risk: Turning Business
Threats Into Competitive Advantage
Reviewed by Reynaldo J. de la Fuente,
CISA, CISM

24
Accounting for Value and Uncertainty
in Security Metrics
By C. Warren Axelrod, Ph.D.,
CISM, CISSP

30
Implementing, Automating and
Validating Controls for Privileged Users
in Healthcare Organizations
By Cheryl Traverse

35
Is the IT Risk Worth a Control?
Defining a Cost-value Proposition
Paradigm for Managing IT Risks
By Sudhakar Sathiyamurthy, ITIL, MCSE

39
New Identity Theft Regulations
By Silka Gonzalez, CISA, CISM, CISSP,
CITP, CPA

42
Issues With Auditing the
Systems Development Process
By Dave Henderson

46
Monitoring Privileged Application Users
in Oracle Applications Environment
By Jeffrey T. Hare, CISA, CIA, CPA

52
Black Box Testing: Its Fundamental
Concepts and Problems
By Pak-Lok Poon, Ph.D., CISA, CSQA,
MACM, MIEEE

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

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

Plus

33
Standards, Statements, Guidelines
ISACA® Member and Certification
Holder Compliance

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


59
CPE Quiz #121
Based on Volume 4, 2008
Kamal Khan, CISA, CISSP, MBCS


S1-S8
ISACA Bookstore Price List Supplement


Online

Online Features

The following articles will be available to ISACA members online on 1 December 2008.

Board Portals: Are They Secure 
By Arvind Godbole, CISA, CA, and Vasant
Raval, CISA

Cibercrimen y Ciberterrorismo: Dos Amenazas Emergentes 
Por Jeimy J. Cano, Ph.D., CFE

Computer Ethics: A Potent Weapon for Information Security Management 
By Wanbil W. Lee, D.B.A., FBCS, FIMA, FHKIE,
and Keith C.C. Chan, Ph.D.

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.

Security University Knows what it takes to be Q/ISP Qualified!
2 Security University Q/ISP Qualified Training Classes!
NYC Dec 5-8, 2008 @ SC World Congress Conference



14,000+ SU
 Qualified Security Professionals
 consistently excel at
 translating tactical security skills
 into secure networks & systems!



Where "Qualified" Happens!



Register Today

Q/SA® Q/PTL® Qualified Security Analyst/Penetration Tester Class & Workshop \$3,495
 90% hands-on labs. Discover vulnerabilities & escalate privileges on multiple complex targets.
 With the Best Pen Testing workshop that qualifies your tactical penetration skills!

Q/EH Qualified Ethical Hacker Class \$3,495
 Hacker tools and techniques to penetrate & attack live targets. The Best in tactical security hacking skills!

*Daily lunch, Online Exam & SC World Congress Conference Pass included in class fees



877.357.7744

www.securityuniversity.net

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 Lead Implementer

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".

For more information, contact us at training@veridion.net



Technology for Business Assurance

LEARN

3 Common fraud tests in under *10 minutes!*

ACL technology gives you greater visibility into virtually everything on the cost side of your business. Our software can help you uncover hundreds of thousands, even millions of dollars a year in inappropriate or duplicate costs, and insure regulatory compliance too.

Visit our new fraud-focused web portal for tips on how **ACL can help prevent fraud at your organization**. You'll find:

- Customer case studies on fighting fraud
- Articles on the principles of fraud detection
- Web seminars on uncovering massive fraud

» Visit www.acl.com/3fraudtests today





**Edge Zarrella,
CA, CISA**

is the global partner in charge of IT advisory at KPMG. Zarrella is also the Asia-Pacific partner in charge of risk advisory services at KPMG, which encompasses the following major service lines: IT advisory, internal audit services, financial risk management, business performance services and accounting advisory services. Zarrella has spent his 20-year career in business and IT advisory. His specializations include IT strategy and governance, sourcing and projects. Zarrella has been an advisor in numerous areas including due diligence in corporate acquisitions, offshoring and outsourcing, and IT strategy.

Guest Editorial

Industry leaders examine
the latest business issues

You Can't Outsource Control

By Edge Zarrella, CISA, CA

Over the years, it has been interesting to note how the term “outsourcing” has moved from an academic idea—to ensure an enterprise’s focus on core business—to a bad word in the press of developed countries, through to what is now seen as a business imperative. Outsourcing has also evolved over these years from outsourcing noncore business activities, which included information technology outsourcing (ITO) through to business process outsourcing (BPO), to the emerging trend of knowledge process outsourcing (KPO), which is effectively starting to outsource the core of a business (see the Evolution of Outsourcing Terms sidebar for definitions of these terms).

When most people think of outsourcing, they automatically think of a call center in India. This is no longer the case. Outsourcing providers can be local, regional or international. (See the Basics of Outsourcing sidebar for more information on the who, what, where, etc.) I have noted several airlines in the US that use home shoring to cover their call center activities, where people in Midwestern America, or anywhere in the world for that matter, can answer phones from the comfort of their own homes. By making use of the time differences as well as skilled staff, small architectural firms are finding value in sending basic design documentation to service providers in another country, who then produce detailed architectural drawings that would have taken their own staff more time at a greater cost. Another emerging trend I have noted is in the medical space, for example, with the interpretation of x-rays and other medical scans. In such a case, scans are taken at a hospital in the US and are e-mailed to a service provider in another country, who produces the detailed medical analysis and returns the findings to the hospital in a timely manner. These examples are miles away from the stereotypical call center in India.

What Does This Mean for IT Auditors?

Outsourcing represents a massive transformation for businesses around the world, and it is imperative to be aware of it and the associated business and IT audit implications. IT auditors need to be aware of how business is changing as a result of outsourcing activities and, from such changes, how this affects the risks in a business and where new controls are required. Accordingly, IT auditors must be flexible in how they assess risks and ensure that they are appropriately covered by the necessary controls.

In this emerging business environment of increased outsourcing activity, ISACA needs to be actively involved in providing guidance on the types of risks to be aware of and the types of controls that can be implemented to mitigate these risks. Further, ISACA can be active in providing guidance to IT auditors on how to perform the assessments of outsourcing activities.

In my global travels, I have noted that in developed countries, such as Australia, the UK and US, the press is reticent to discuss outsourcing. Enterprises have noted that it is not popular to publicly acknowledge outsourcing activities as there is a widely held, incorrect perspective that outsourcing takes local jobs away. This is not entirely correct; by outsourcing certain activities, there still remain higher value activities that need to be managed and monitored, such as client relationships that need to be managed and face-to-face activities that cannot yet be outsourced.

Governance and Control

Often when enterprises outsource their activities, they think that when something has been pushed to another enterprise, with a legally binding contract and monthly/quarterly

relationship meetings, the activity that has been outsourced will be looked after as they would have if they had not sent it elsewhere to be done. Further, there is sometimes the expectation that the third-party service provider will actually perform the activity better due to the many examples cited in their pitch to do this work. What often gets revealed as a result of process failure is that the third-party service provider does not have the same standard of controls as the originating enterprise. However, often, when this is identified, the problem is already systemic.

It is important to understand that an enterprise cannot outsource control. It is still ultimately responsible for the governance of its business activities. An enterprise can outsource the activity or the process, but its risk appetite may be different from that of its third-party service provider. Just as in any relationship, it is important to establish the enterprise's expectations of the third-party service provider at the outset, to ensure alignment of interests. As such, it is important to look at the end-to-end process the enterprise is outsourcing, and ensure that the controls the enterprise expects to have are controls the third-party service provider is required to implement to fulfill its governance obligations to the originating enterprise—the paying customer.

Alongside the right to audit, processes should be put in place to check that the controls the enterprise has asked the third-party service provider to implement have indeed been implemented, are operating as designed and are effective.

When the outsourcing relationship is set up, it is important to be aware of cultural, technology and communications challenges. Critical in this is to ensure that the controls are covered and monitored. There are third-party assurance reports, in the form of the American Institute of Certified Public Accountants' Statement on Auditing Standards (SAS) 70 (a US standard, which is quickly becoming the *de facto* standard globally for third-party reviews and opinions). These are independent reports that are designed for distribution to stakeholders.

Successful outsourcing activity is not usually defined by a contract, but by happy relationship people. The relationship managers from the originating enterprise and the third-party service provider are critical people in this arrangement.

Emerging Economies and Changing Demographics

In my travels, I have noticed that many of the developed economies have rapidly aging populations; governments of these countries are starting to recognize their aging populations and consider how this will affect their country's competitiveness on the global stage. The emerging economies have the opposite issue and are custodians of the education of this large pool of young talent. IT auditors should be actively involved in ensuring that the young talent in emerging economies is not misdirected, and that it is equipped with strong skills to work in the new business environment.

There is a significant increase of activity in the emerging economies of Latin America, Central Europe, Malaysia, Vietnam and China. Many outsourcing companies are considering options to increase their presence in these locations. IT auditors need to have a strong understanding of how information flows move across the more developed to the emerging countries. They need to have a strong understanding of the regulations, laws and rulings in the emerging countries.

Evolution of Outsourcing Terms

Knowledge process outsourcing (KPO) enables clients to unlock their top-line growth by outsourcing their core work to locations that have a highly skilled and relatively cheap talent pool. KPO is about intellectual arbitrage and is characterized by niche offerings, highly skilled staff and a relatively small scale; it cuts into the traditional core competencies of many organizations.

Business process outsourcing (BPO) enables clients to outsource noncore, back-office, repeatable, high-volume, low-value transactions. This focuses on cost arbitrage.

Information technology outsourcing (ITO) enables clients to outsource technology-related activities. It could include data center hosting and management services, code development, and any aspect of IT management. This also focuses on cost arbitrage.

Outsourcing Basics

Who—Everyone is involved (even if they say they are not).

What—No longer just noncore, back-office, repeatable, high-volume, low-value activities. By examining the evolution of outsourcing, it is evident that BPO is a more advanced form of outsourcing than ITO, and KPO is a more advanced version of BPO. KPO taps into the core of a business.

When—In varying degrees of maturity in different locations over many years

Where—Everywhere. There are countries that outsource, and countries that provide services. This is not limited to India; other emerging destinations providing outsourcing services include Malaysia, Vietnam, Canada, Latin America, Eastern Europe and Southeast Asia.

Why—These activities are undertaken for strategic advantages, cost savings and process improvements.

How—Some organizations are undertaking outsourcing activities themselves, some have sought external assistance and some are being fully guided through outsourcing activities.

Success rate—Varying degrees

I am a strong believer that as time progresses it will be necessary to recruit, retain and develop IT audit professionals in these emerging markets to take on and carry out the audits that are required on these outsourcing/offshoring enterprises. Flying people in and out is not conducive for efficiency and effectiveness. This is going to be a major challenge for IS auditors going forward. IS auditors will need to drive growth and professionalism in these markets, which will become the major economic powerhouses of the future.

GEARED FOR SUCCESS?



Don't hit the brakes. Renew your ISACA® membership and continue to accelerate your career.

As an IT audit, security or governance professional, increase your professional mileage and master the road ahead.

ISACA fuels your career through:

- **Professional development:** Get a professional edge, broaden your perspective, fine-tune your skills and earn CPE credits.
- **Research and knowledge:** Stay up to date with the latest thought leadership, best practices and professional resources.
- **Community and leadership:** Connect with a global community of more than 86,000 constituents.

ISACA membership will continue to help drive your career to the next level.

Renew your ISACA membership today!

www.isaca.org/renew



Innovation. Be a part of IT.



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

**or call Cyber-Ark Software on
888 808 9005**



The Leader in Privileged Identity Management Solutions



Certification and the Disappearing Perimeter

By Steven J. Ross, CISA, CBCP, CISSP

It is not a particularly original observation that perimeter security of information systems is no longer effective.¹ There was a time, or so I seem to recall, that systems could be protected by allowing authorized users within a company to access the information on its computer system, but prevent outsiders from doing so. I speak of the system in the singular, because at that time, all information was contained in a centralized, mainframe environment, around which it was possible to build a virtual wall, keeping known users within and everyone else outside.

Today, both business conditions and the underlying technology that supports them have changed. Centralized mainframes have given way to distributed technologies. Concurrently, many companies have decomposed their business processes and turned some parts of the processes over to other companies, i.e., they have outsourced some of their operations. As a result, it no longer makes sense to prevent outsiders from having access to an organization's systems and information; in fact, outsiders are invited in. Moreover, the collaborative nature of 21st century business means that competitors often share some business activities—in joint ventures, combined research, strategic alliances and other shared enterprises. Now, not only are strangers allowed within the gates, so are some enemies!²

Add e-commerce to the mix and we see customers, in addition to vendors, having access directly to their suppliers' systems, entering their own orders, monitoring the progress of those orders (and often of the manufacturer of the goods themselves) and generally taking advantage of the Internet to intertwine their own operations and systems with those of the vendor. To continue with the unoriginality of the first sentence, the Internet has changed everything.

Establishing Trust

The disappearing perimeter has necessitated a variety of approaches to securing information, among them firewalls, compartmentalization and identity management. It has been my experience that these controls are effective, as long as the host systems are administered with a complete knowledge of the access entitlements of employees, contractors and remote third parties. However, it is a rare company that has anything close to a complete knowledge of the interactions among applications, infrastructure, data and users.

As a result of the blurring of boundaries among businesses and their IT environments, organizations are looking for reassurance about the security, recoverability, reliability and internal controls of the third parties with whom they are connected. Inherent in the complex interactions among vendors, customers, joint venturers and even competitors is *trust*.

The conundrum for these organizations is that while they are confident that they themselves are trustworthy, they are not so certain about the others. They would like to peer into others' data centers but are leery of anyone looking into their own affairs. A number of solutions have presented themselves in the past:

- In my experience, the most common approach is blind faith, a tacit policy of "don't ask, don't tell." This may be recognition of a situation in which one party lacks the influence over another to obtain anything more than vague assurance that security is adequate, without substantiation to support this assertion. If, for example, a company is reliant on a sole vendor of a unique product, there is little room for insisting on auditable evidence.
- In more equal relationships, one or both parties may obtain a contractual right of audit, which allows the auditors of one company to inspect, to a greater or lesser degree, the security of the other. Of course, such an arrangement is sensible only for very meaningful interactions—it would be quite obtrusive to have numerous examinations from multiple sources.

What Certification Is

Into the gap comes certification, a process by which an organization can be certified for adherence to specific standards. The best known of these in the security sphere, on an international basis, is the International Standard ISO/IEC 27001:2005, which is based on the British Standard (BS) 7799 and was published in October 2005 by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC), and, more recently, BS 25999-2:2007. ISO 27001 (as it will be referred to here for ease of reference) is the certifying standard for ISO/IEC 27002:2005, which is the code of practice for information security management. The nomenclature seems certain to have been designed to confuse, but, suffice to say, this pair of standards is internationally recognized as an information security baseline. BS 25999 relates to business continuity management (BCM). While not actually applicable outside Great Britain, it has rapidly attained worldwide respect as a point of reference, if not a standard.³

Without going into the arcana of the certifying process, a company wishing to be certified submits documentary evidence to BSI British Standards, the National Standards Body of the UK, validating that it adheres to the 11 security control clauses and their dependent security categories for ISO 27001 certification or the six clauses of BS 25999 for certification of its BCM program. Once the documentation

is reviewed for indication of adequate adherence to the appropriate standard, BSI performs an onsite audit before issuing a certificate. The audit is repeated every several years for recertification. Thus, the company in question can claim to be ISO 27001- or BS 25999-certified. Most important, in the context of the disappearing perimeter, other companies can have some basis for trust in the security or recoverability of the certified organization with which they do business.

Inasmuch as the standards in question have, to a greater or lesser degree, international recognition, certification against them carries weight around the world. ISO 27001 or BS 25999 certification is a benchmark of trustworthiness that may be a part of the glue that will hold an extended enterprise together.

What Certification Means

Certification is not an unbounded assurance of security or recoverability. Any individual or organization wishing to place reliance on an associated business's certificate must understand exactly what is certified. Certification may extend to an entire enterprise, but it also may be limited to a division, a specific premise or a data center.

Moreover, ISO 27001 certification does not, in itself, mean that a company is secure, nor does BS 25999 certification mean that it is recoverable. The certifications indicate that the organization in question has followed a process that would—perhaps should—lead it to be secure or recoverable. This narrow distinction does not invalidate the basis of trust, but it does require associated parties relying on a certificate to understand exactly what they are relying on.

In an odd way, the words certificate and certification carry a double meaning in information security. Aside from validation of adherence to a standard, a digital certificate is the central element of a public key infrastructure (PKI). In both cases, a third-party certifying organization may be inserted in commercial relationships to create a basis of trust. Both have strengths and limitations, and both are essential to the evolution of a business world of extensive electronic interaction.

Endnotes

¹ See “The Vanished Perimeter,” *Information Systems Control Journal*, volume 5, 2003.

² The term for this, “coopetition” is attributed to Novell's Ray Noorda. See Brandenburger, *et al.*, *Coopetition*, Doubleday, 1998.

³ It is only fair to note that some individuals and trade organizations reject BS 25999, and point to other standards such as the American NFPA 1600 or the codes of practice of some of the business continuity management certifying bodies for professionals in the field. The issue is to an extent moot in this case in that the issue concerns the certification, not the standard.

Steven J. Ross, CISA, CBCP, CISSP

is a director at Deloitte. He welcomes comments at stross@deloitte.com.



Manage your risks and show due diligence to customers & stakeholders

Modulo Risk Manager™ provides an integrated solution for:

- Compliance with SOx, PCI DSS, ISO 27001, ISO 27002, CobiT, BS 25999, HIPAA, FISMA, NIST 800-53a, A130, ITIL, ISO 20000, DOD 8500.2, Basel II and more
- Automating risk management and remediation progress measurement
- Centralized, consistent and comprehensive analysis of risk policies and controls
- Eliminating costly redundancy and reducing audit silos
- Incident, remediation and Business Continuity Management



Modulo: global leader in
**IT Governance, Risk and
Compliance Management**

Contact us for a presentation!

www.modulo.com | Toll free: **866-663-5802**

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**

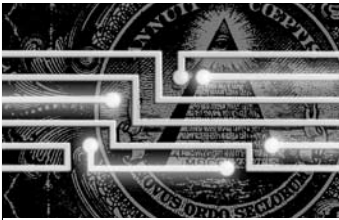
INTERNAL AUDIT SOFTWARE • THINK PAISLEY

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**



IT AUDIT BASICS

What Every IT Auditor Should Know About Auditing Virtual Machine Technology

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

is an associate professor of information systems (IS) 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 IS using microcomputers. Singleton is also a scholar-in-residence for IT audit and forensic accounting at Carr Riggs Ingram, a large regional public accounting firm in the southeastern US. 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, IT/IS, IT auditing and IT governance have appeared in numerous publications, including the *Information Systems Control Journal*.

Moore's Law—which states that the number of transistors on a given chip can be doubled every two years—has been the guiding principle of progress in electronics and computing since Moore first formulated the famous dictum in 1965.¹ During the time since, chips and computers have become simultaneously more powerful and less expensive. In some markets, “you can get 50 million transistors for a buck these days,” Moore said. In the late 1950s, some chips had 200 transistors; by 2005, Intel produced chips with 1 billion transistors. Semiconductor industry revenue has grown 800-fold since the late 1950s. There is little doubt that not only has Moore's Law become a reality, and not only has it stood up for four decades, but it also appears that it will be sustained for at least one more.

It also is the driving force behind the creation of most of the new hardware technologies over the last four decades. Those advances have led to new major technologies at least every three to four years. One of those new technologies is Virtual Machine (VM). Although IBM has had VM technology since about 1972, it is only recently with the more powerful and less-expensive servers, and the development of new VM tools, including IBM's newest Z-series mainframes, that VM has become a significant cost-savings technology. By the end of 2007, 75 percent of companies with 1,000 or more employees were using virtualization technology. But, by 2009, it is estimated that 60 percent of production VMs will be less secure than physical counterparts.²

A Virtual Machine, the hardware type vs. the software type,³ allows multiple operating systems (O/S) to coexist on the same machine in isolation from one another, to avoid conflicts and inoperability. Thus, several single-task O/S can operate simultaneously on a single server (computing machine). The O/S can be different, even incompatible. There is an obvious efficiency outcome, both in

money spent on server hardware, but also in the concomitant space needed, maintenance of hardware, and other service costs of hardware. Altogether, companies can save a significant amount of costs by switching from server farms to VMs.

It could also be configured to handle multiple partitions of the same O/S to avoid similar problems. For example, untested code can be tested and debugged in its own VM partition, isolated from operating code in another partition on the same server, thus preventing the untested code from causing operational problems. This configuration also saves costs in establishing an adequate testing environment. The untested partition (VM) acts as a staging area or sandbox. This configuration would be a best practice, testing code thoroughly and safely before it becomes operational. VM is often configured to handle special software services, such as XML or Web Services, and pass the data on through to operational applications and databases that may exist on the same server.

In some respects, moving from a traditional server machine to a virtual machine is somewhat like moving from a single computer to a network of computers. The primary difference is one of exponential increase in risks associated with scope (points of access, opportunities for nefarious activities, etc.).

It is also true that auditing a VM server is similar to auditing any server. According to experts, the same principles, best practices and basic audit approach should be used for a group of VMs as for a server farm. IT audits should, and do, use past experience with traditional servers on audits of VM servers.

However, there are some proprietary facts about VM. For example, VM tools are different from the traditional server tools; it takes only minutes to establish a new VM server (compared to hours or days for a physical server).

This article attempts to outline those aspects that are similar, and the unique

aspects of VM that every IT auditor should know when auditing VM technology. The focus of this article deliberately excludes tools in favor of providing the basics of what IT auditors would need to know and do with or without VM tools.

Risk Assessment

Virtually all types of audits in today's world begin with a risk assessment. Audits of VM are no different. But the IT auditor needs to understand the peculiar risks associated with VM. The main concerns are how IT resources are separated and aggregated in a VM environment, and how the VM environment security is managed.

For instance, the fact that several partitions normally are physically located on a single server increases the risk of malicious activities. In a "regular" host/server of the past, if an attack occurred, it would normally be restricted to the data on that machine. In VM, an attack could penetrate several different databases located on various VMs on the host machine. Thus, the risk of malicious attack in VM is greater due to scope.

The same is true about administrative access to the host machine. Because administrative (admin) rights could affect all partitions, the management console needs to have tight access controls, locked down to specific users and specific partitions or machines. Once access is gained, the person with admin rights could gain access to any of the databases or applications in any of the several partitions. A typical mistake in VM management is to allow too much access to users, for example, a developer given admin rights to a VM partition.

Understand the System

Another key and common ingredient to audits is gaining an understanding of the technologies and/or systems to be audited. That is, of course, true for VM as well.

As with any network, the IT auditor should gain an adequate understanding of the infrastructure and how controls are embedded, or overlaid upon, the partitions and server(s):

- Are the partitions different operating systems?
- Are the partitions on a single server or across servers?
- What partitions exist for which environments on which boxes (i.e., a network map)?
- Are there controls over each partition similar to those expected for a server?
- Are there controls for specific users that limit access and read/write capabilities?
- Does a standard naming convention exist, and, if so, what is it—for server, partition, library/folder names? These, of course, help IT auditors perform their duties.
- What controls are in place for deploying multiple copies of software (maybe thousands!)?

The implications should become intuitive from these questions. If the partitions are on the same host server, and if the configuration (e.g., password policy) has control deficiencies, then that single control deficiency actually affects multiple virtual servers (partitions). The same is true for faulty admin access—it affects multiple virtual servers.

Thus, the impact of the control deficiency is greater than it would be for a traditional physical server.

The opposite is also true. If the entity has employed the best practice of centralizing management of multiple environments using some appropriate standards, it may have chosen to simplify the application of its policies by employing VM to manage multiple environments from a single access control.

The understanding of the VM environment and subsequent evaluation and testing of controls will likely focus on the network map. The IT auditor should determine where in the VM world the following types of systems are located, if they exist:

- Systems development
- Systems testing (staging or sandbox environment)
- Production systems (the larger the company, the more of these will exist)
- Regional business unit servers (if applicable)

Last, the IT auditor should be able to evaluate the completeness and accuracy of VM documentation. For

instance, the IT auditor would want to evaluate/test change controls. In the VM world, the IT auditor needs to make sure the documents for change control being validated are from the right partition and on the right server. It is also necessary to know with certainty how to determine completeness and accuracy of the change documentation.

The bottom line is that the IT auditor needs to be able to evaluate the process of creating, deploying, managing and making changes to virtual machines.

Best Practices

As always, the IT auditor should be aware of some of the best practices as a benchmark for effectiveness of controls, operations and business processes. There are guides for VM, such as the Center for Internet Security, the Defense Information Systems Agency and server leader VMware.⁴ IT auditors should obtain a copy of these and read them. They can provide a summary set of lock-down and hardening policies that are customized for the various environments that might exist in VMs.

IT auditors should then use those best practices as a baseline and during the audit, and on subsequent audits, make sure the controls over the virtualization layer have not "drifted."⁵ One way to avoid drift is to keep patches up to date—a well-known best practice for servers and networks. The IT auditor needs a way to evaluate the currency of relevant patches to the VM.

The IT auditor would check for best practices of traffic from one server to other servers, and from server to external devices. IT auditors would evaluate the sufficiency of controls such as a (virtual) firewall and (virtualized) intrusion detection system, where applicable. A developing best practice is to exclude the use of VM in the DMZ (the layer between the Internet and the entity's LAN).

A primary concern, as mentioned above, is that of the management console. Best practice calls for management tools to run on a separate network. Such a configuration has the potential to prevent VMs from prying into the console communications with which it is trying to control the VM.

*The risk of malicious
attack in VM is
greater.*

A similar best practice is the hypervisor, the software tool that houses the VM servers. There is an embedded type of hypervisor that comes with the physical VM and is not part of a general purpose O/S. VMware's embedded hypervisor is only 32 MB (skinny by comparison; and the smaller the code, the safer it is from breaches). This, combined with the fact that it is not part of an O/S, increases the security of the hypervisor.

Conclusion

Much of what the IT auditor does in an audit of VM is to apply what works effectively in audits of physical servers. However, the IT auditor should consider evidence and assurance regarding controls over those unique aspects of VM. IT auditors should, therefore, become aware of best practices in VM. By using basic IT audit techniques, and applying them to special circumstances that exist in the VM world, the IT auditor will be able to provide the same quality audit as those of physical servers.

Endnotes

- ¹ Moore, Gordon E.; "Cramming More Components onto Integrated Circuits," *Electronics Magazine*, 19 April 1965
- ² Per Gartner Group Vice President Neil MacDonald, as quoted in: McLaughlin, Laurianne; "How to Find and Fix 10 Real Security Threats on Your Virtual Servers," *CIO Magazine*, 14 November 2007, www.cio.com/article/print/154950
- ³ There are process VM that create temporary VMs to support a process, from software that "evaporates" when the process is completed. Sun uses Java Virtual Machine, and Microsoft uses Common Language Runtime in its .NET environment. Both of these are examples of process, or software, VM.
- ⁴ Silwa, Carol; "Audit and Improve Virtual Server Security: Five Tips," *CIO Magazine*, 7 May 2008, www.cio.com/article/print/351013
- ⁵ When changes cause subsequent versions of the VM configuration to be removed somewhat from best practices, it is known as "configuration drift."

S E R V I N G I T G O V E R N A N C E P R O F E S S I O N A L S



EuroCACS Conference

"The World's Leading Conference for IT Audit, Security and Governance Professionals"

Innovation. Be a part of IT.

15-18 March 2009
InterContinental Frankfurt
Frankfurt, Germany

Conference Highlights:

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



Earn up to **40** CPE Credits.

Register early and receive a discount on conference registration fees!

www.isaca.org/eurocacs

★ Celebrating ★

30 YEARS

*The Nation's Premier Recruiting Firm
for the Audit Profession*

LANDER

INTERNATIONAL, LLC

Honesty

Integrity

Ethics

The strongest audit departments around the world depend on
Lander International to find the talent they need.

The best auditors trust Lander International to find them premier
career opportunities.

(800) 548-5318 in USA and Canada

(510) 232-4264 International

www.landerint.com

Phishing and Countermeasures:

Understanding the Increasing Problem of Identity Theft

Edited by Markus Jacobsson and Steven Myers

Reviewed by Vishnu Kanhere, Ph.D., CISA, CISM, AICWA, CFE, FCA

Phishing has become a universal phenomenon and a major threat worldwide that affects all industries and businesses that have an online presence and provide online transactions on the Internet. In fact, progressively, phishing is being resorted to, not by novice hackers and crackers, but by organized criminal gangs to exploit Internet users in a systematic way.

A comprehensive source of reference, organized into 19 chapters and an index, *Phishing and Countermeasures* is put together in such a way that readers with some exposure to computers and computing will be able to understand and use it, without the need for any expert technical knowledge of the subject. The chapters have sufficient definitions, technical expositions, figures, charts, screenshots and tables to provide the necessary detailing.

The book aims to lay the foundation for understanding phishing and devising antiphishing techniques. Phishing is equal parts technology and psychology. Educational campaigns create awareness among users and help in the fight against phishing. The authors feel that these do not necessarily have a long-term benefit, as phishers are also educated by these campaigns and quickly learn how to tailor their baits so that users do not recognize them. To really understand phishing, one needs to wear the “hat” and put oneself into the “shoes” of the hacker/phisher and, short of actually victimizing people, should actually try phishing measures so that appropriate countermeasures can be developed using technology.

The first four chapters give an overview of the problem of phishing. The fifth chapter outlines some of the common countermeasures. Chapter six discusses spear phishing that infers or manipulates the context of the victim before mounting an attack. Chapter seven brings out mistakes that an average computer user can and will make and their impact on system design. Chapters eight, nine and 10 describe techniques of how machines can identify humans and their identity. Chapter 11 describes distributed phishing attacks that make the takedown of all involved web sites, following discovery, extremely difficult.

Chapters 12 through 15 describe security measures associated with browsers. Chapter 16 highlights problems associated with the use of certificates and how users react to them. Chapter 17 gives insight into assessments of risks associated with threats and the methods used to assess the benefits of security tools in these situations. The legal aspects and issues concerning phishing, in the US context, are discussed in chapter 18.

Finally, chapter 19 gives an overview of the future. Currently phishing attacks are primarily mounted using e-mails, but it is quite likely that these will spread to other messaging techniques, such as instant messaging, Short Message Service (SMS) and text/image-based messages, and Voice-over Internet Protocol (VOIP).

In such a scenario, the only logical way to counter phishing seems to be to rely on the triad of technology, legislation and awareness:

- **Technology**—To counter phishing attacks and make them difficult to mount
- **Legislation**—Made more stringent to deter such attacks by making them less worthwhile if discovered
- **Awareness of the users**—So that a lesser and lower number of people fall prey to them, thereby frustrating those involved in phishing

The large numbers of contributors and their inputs, ably assembled and presented in this book, make this useful for computer scientists, information systems (IS) auditors, security professionals, students, researchers, law and policy makers, software developers, and system designers.

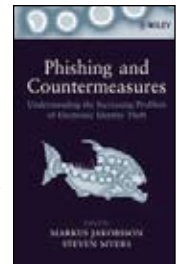
Vishnu Kanhere, Ph.D., CISA, CISM, AICWA, CFE, FCA is an expert in software valuation, IS security and IS audit.

A renowned faculty member at several management institutes, government academies and corporate training programs, Kanhere is a member of the Sectional Committee LITD 17 on Information Security and Biometrics of the Bureau of Indian Standards. He is currently newsletter editor, academic relations, standards and research coordinator of the ISACA Mumbai Chapter; member of the ISACA Publications Committee;

honorary secretary of the Computer Society of India, Mumbai Chapter; convener of a special interest group on security; chairman of WIRC of eISA; and convener of the security committee of the IT cell of Indian Merchants' Chamber. He can be contacted at vkanhere@vsnl.com or vishnukanhere@yahoo.com.

Editor's Note:

Phishing and Countermeasures: Understanding the Increasing Problem of Identity Theft is available from the ISACA Bookstore. For information, see the ISACA Bookstore Supplement in this *Journal*, visit www.isaca.org/bookstore, e-mail bookstore@isaca.org or telephone +1.847.660.5650.



*Phishing is equal
parts technology and
psychology.*

IT Risk: Turning Business Threats Into Competitive Advantage

By George Westerman and Richard Hunter

Reviewed by Reynaldo J. de la Fuente, CISA, CISM

This book fills an existing gap, addressing IT risk in a friendly way, making it possible to tackle the subject without having to cope with tough and complex risk quantifications. It provides the necessary knowledge and focus on risk management to support the study of domain four of the Certified in the Governance of Enterprise IT™ (CGEIT™) certification job practice for those considering the CGEIT exam.

The book approaches IT risk not as a technical issue, but as a business and management one. It can be thought of as being split in three parts. Part one is about the framework and the overall approach to risk management. Part two concentrates on the actionable management steps business and technology executives can use to manage risk. Part three looks at the future and proposes improvements to risk management.

Part one includes the following chapters:

- **Chapter 1: The 4A Risk Management Framework**—The authors introduce here a framework of four A's that looks at risk from a business perspective, rather than an assurance or compliance perspective. The four A's that define IT risk are:
 - Availability—Keeping business processes and information flowing through the business
 - Access—Ensuring that the appropriate people, including customers and suppliers, can get the information and functionality they need to be effective
 - Accuracy—Concentrating on providing timely and complete information to meet operating and oversight needs
 - Agility—The ability to change with managed cost and speed
- **Chapter 2: The Three Core Disciplines of IT Risk Management**—These are:
 - A well-structured foundation of IT assets, an installed technology base of infrastructure and application technologies, and supporting personnel and procedures
 - A well-designed and well-executed risk governance process that provides an enterprise-level view of all risks
 - A risk-aware culture in which everyone has appropriate knowledge of risk

Part two includes the following chapters:

- **Chapter 3: Fixing the Foundation**—Strengthening the base of the pyramid; the importance of infrastructure in risk management
- **Chapter 4: Fixing the Foundation**—Simplifying the base of the pyramid; about how complexity drives risk, cost and performance levels. The authors make a critical point when they show how change in infrastructure is IT change, while change in applications is business change.
- **Chapter 5: Developing the Risk Governance Process**—Covering how to manage and make decisions regarding IT and business risks

- **Chapter 6: Building a Risk-aware Culture**—The authors make an important connection between risk and culture, and a critical distinction between being risk-aware and risk-averse.
- **Chapter 7: Bringing the Three Disciplines up to Speed**—Concentrates on the program and patterns for effective implementation

With the tools of chapter four and the scenarios of chapter six, the authors have built a good example of a midsized company finding its legacy applications—and the lack of agility in them—to be a key risk, and the need to invest in replacing and upgrading systems to make maintenance and evolution easier and less risky.

Part three includes the following chapters:

- **Chapter 8: Looking Ahead**—Talks about how to incorporate risk management as a positive force in planning and strategy setting
- **Chapter 9: Ten Ways Executives Can Improve IT Risk Management**—The book closes with a brief reminder of different ways executives can improve IT risk management. Some of these ways are:
 - Treat IT risk as business risk.
 - Simplify the foundation.
 - Give to every employee an appropriate awareness of the risks, vulnerabilities and policies that matter most to them.
 - Measure effectiveness.
 - Lead by example.

Overall, this is a must-read for chief information officers and IT risk management and IT governance professionals. It is also recommended reading for chief executive officers (CEOs) and others who want to understand how to manage IT risk.

Reynaldo J. de la Fuente, CISA, CISM

is CEO of Datasec (www.datasec-soft.com), an IT governance, security and assurance company in Uruguay specializing in *ad hoc* software development. He was recognized with ISACA's 2005 John W. Lainhart IV Award for outstanding contribution to developing the profession's common body of knowledge. He has served in several ISACA chapter and international positions since 1993.

Editor's Note:

IT Risk: Turning Business Threats Into Competitive Advantage is available from the ISACA Bookstore. For information, see the ISACA Bookstore Supplement in this *Journal*, visit www.isaca.org/bookstore, e-mail bookstore@isaca.org or telephone +1.847.660.5650.



Practical Guidance on Establishing the Val IT Value Governance Process

By Sarah Harries and Peter Harrison, FCPA

This is the third 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 previous two articles (found in volumes 3 and 4 of 2008) described how to recognise the need for Val IT and five basic steps for introducing Val IT.

The remainder of the series will cover:

- The Challenges of Implementing Portfolio Management
- Benefits Realisation and Programme Management—Beyond the Business Case
- Critical Success Factors for Introducing Val IT

Implementing Val IT in an established, complex enterprise is not necessarily easy. Is it worth it? Well, if the enterprise wants to get the maximum business value from its IT-enabled investments—yes! But, where does one start? Addressing the Value Governance (VG) process first is the ideal answer, because VG establishes the governance framework on which the other two domains of Val IT, Portfolio Management (PM) and Investment Management (IM), depend.

This article describes six typical issues that might be encountered when implementing VG and offers practical guidance on how to overcome them.

Typical Issues in Implementing VG

The typical issues in implementing the VG process include:

- **Underestimating the emotions and politics involved**—Governance is a touchy subject; it is about the power structure of an enterprise and the individual behaviour expected within that structure. Humans are naturally resistant to behavioural change, especially if they have not bought into the reasons for it. Whatever changes are proposed will not be accepted and certainly cannot be sustained, unless there is backing and sponsorship at the highest levels. This is also necessary because most of the significant issues that need tackling run across multiple areas of the enterprise and cannot be solved by lower levels of management.
- **Assuming who calls the shots**—Val IT calls for clear and active linkage between the enterprise strategy and

the portfolio of IT-enabled investment programmes.

Decisions on what should be included in the portfolio of active investments may be fragmented between the chief information officer and business executives, who may each make assumptions regarding how and by whom decisions should be made.

- **Designing in isolation**—An enterprise's governance framework is rarely holistic but rather a mishmash of elements operating in silos. It may well have evolved over time, in a rather piecemeal fashion, with policies and processes sporadically implemented to address specific *ad hoc* issues or requirements.
- **Ignoring established and successful methods**—Enterprises that exist, particularly those that have grown and succeeded in difficult markets, must be doing something right. To suggest that well-established, tried and tested methods and approaches should be cast out in favour of new ones will be a hard message to sell to the stakeholders.
- **Thinking about reports, but not what is done with them**—Governance is about getting the right information to the right people at the right time to enable them to make the right decisions. It is easy enough to design a new report, create a board to scrutinise it and organise a meeting at which they discuss it; however, change happens only when actions follow the board's decisions.
- **Assuming the enterprise will stand still**—Markets change and so must strategy if the enterprise wants to keep up with the changes. Even in the public sector, policies are constantly changing, as do the department's spending priorities. Governance needs to support the enterprise; it must contain adequate controls to avoid exposure to unacceptable risk, yet it must be lean and easy to change. This last point is critical if the enterprise needs its governance to support agility rather than prevent it.

How to Avoid the Pitfalls

The following actions can help one avoid the pitfalls of the VG implementation process:

- **Acquire senior sponsorship**—The most significant factors contributing to the poor take-up of good governance are denial and internal politics. Governance arrangements need to be seen by all stakeholders as value-creating, rather than distracting

resource burners. If senior key stakeholders can see how the changes proposed will make their own jobs easier, it is much more likely that their sponsorship will be acquired, which will also help to enforce and sustain the proposed changes.

- **Ensure alignment between business planning and service management planning**—The governance framework should include a board that fulfils the role of an IT strategy committee (see COBIT) or investment and services board (see Val IT). These would include senior representation from the business functions and the IT function (and major suppliers, if applicable), so that strategic direction of the enterprise can be discussed and the overall strategy of the IT service aligned with it.
- **Ensure appropriate accountability, apply the rule of subsidiarity**—Keeping the governance lean does not mean having as few controls as possible; rather, it means designing it in such a way that decisions can be made at the most appropriate level. Essentially, nothing should be done at a higher level that can be done as well or better at a lower level.
- **Develop the governance framework from the top down**—This is especially true of enterprises that have disparate business units or geographies, as they are likely to have established silos and layers of governance. Understand the scope (breadth) of the changes to governance required and then start at the top layer. Senior stakeholder sponsorship is vital in all the areas that are currently regarded as autonomous; otherwise, the change will be impossible to sustain.
- **Consider all the dimensions**—In scoping out the changes required for governance, ensure that all the dimensions of change are considered: business, technology, organisation, people and processes. Remember that some changes will affect dealings with external enterprises, so plan for appropriate communications.
- **Keep what works**—Find ways to introduce small changes at first, such as eliminating duplicated responsibilities in the various boards and forums, to enhance and improve existing systems. This will be much easier to enforce and subsequently build on, than starting from scratch. It will also help to win over internal stakeholders to support the wider-scale changes that follow.
- **Define end-to-end reporting requirements**—Reports should also be documented, with their typical contents, frequency, author/owners and recipients. Decisions that are made by these governing bodies and any actions allocated, should be recorded and communicated back to the appropriate people and, where relevant, accepted by them as actions or incorporated into the relevant plans (e.g., programme plan, service improvement plan, change plan).
- **Document and communicate roles, responsibilities and accountabilities**—Accountability for the VG process itself must be allocated. The VG process owner will be responsible for ensuring that as much as possible is documented and communicated to the right people. Documentation is important if new stakeholders need to be informed, responsibility needs to be passed on, rules need to be enforced, or changes need to be made and agreed upon.
- **Plan for more change**—Make sure there is a process in place to assess periodically the effectiveness of the governance framework, and to change it where necessary.

The minimum frequency should be annually, and reviews should always assess whether any processes can be made more 'lean'.

Figure 1 provides a breakdown, process by process, of the typical issue and steps to avoid in establishing the VG process.

Figure 1—Implementing Val IT Processes to Overcome Typical Issues

Establishment of Value Governance (VG)		
Typical Issues	Steps to Avoid These Issues	Val IT Framework 2.0 Processes
<ul style="list-style-type: none"> • Underestimating the emotions and politics involved • Assuming who calls the shots 	<ul style="list-style-type: none"> • Acquire senior sponsorship. • Ensure alignment between business planning and service management planning. • Ensure appropriate accountability. 	<ul style="list-style-type: none"> • VG1
<ul style="list-style-type: none"> • Designing in isolation 	<ul style="list-style-type: none"> • Develop the governance framework top-down. • Consider all dimensions. 	<ul style="list-style-type: none"> • VG1 • VG2 • VG4 • VG5
<ul style="list-style-type: none"> • Ignoring established and successful methods 	<ul style="list-style-type: none"> • Keep what works. 	<ul style="list-style-type: none"> • VG2
<ul style="list-style-type: none"> • Thinking about reports but not what is done with them 	<ul style="list-style-type: none"> • Define end-to-end reporting. • Document and communicate roles, responsibilities and accountabilities. 	<ul style="list-style-type: none"> • VG5
<ul style="list-style-type: none"> • Assuming the enterprise will stand still 	<ul style="list-style-type: none"> • Plan for more change. 	<ul style="list-style-type: none"> • VG6

Editor's Note

Readers are encouraged to review Val IT (www.itgi.org/valit), as described in *Enterprise Value: Governance of IT Investments*, *The Val IT™ Framework 2.0* and *Enterprise Value: Governance of IT Investments, Getting Started With Value Management*, and share it with key governance stakeholders within their enterprises.

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 Enterprise Value Management leadership team within Fujitsu Consulting Australia and New Zealand, and is a member of the Val IT Steering Committee.



Five Questions With...

Antonio F. Pecora, CISA, CISM, CGEIT, CRP, CFS, CPM, ISSPCS



Antonio Pecora is a partner in the consulting practice and leader of the information management service line in Deloitte Mexico. His principal areas of expertise include data governance, IT security and risk management, and computer audits, primarily in the financial, manufacturing, retail and government sectors. He has more than nine years of experience establishing and creating security governance strategies and information security implementation plans for large organizations as well as designing, developing and managing information security programs for applicable laws and regulations. Away from the office he enjoys playing tennis and soccer, spending time with his family, and reading books by his favorite author—William Walker Atkinson.

Question

What are the effects of corporate governance, risk management and compliance pressures on corporate data?

Answer

The effects of corporate governance, risk management and compliance pressures on the management team of an enterprise have been oft publicized. It is foolish, however, to assume that these pressures start and end in the boardroom. Database professionals face similar pressures in choosing and maintaining the systems and processes that will help protect the integrity of corporate data.

Information (data) can be a company's most valuable asset, and properly protecting the data is often a common element in addressing challenges related to governance, risk and compliance. Data auditing is a primary means for protecting corporate data assets against potential risk and loss. It provides an unimpeachable record of corporate data use, allowing enterprises to validate compliance and implement key practices to ensure that the company operates at the very highest levels of ethics and compliance. Data auditing is key to identifying potential legal threats, because it provides a transparent view of the evolution of information upon which corporate financial reports and other corporate legal documents rely.

Question

How can you simplify the massive task of data auditing?

Answer

When considering the quantity of electronic data within each organization, data audits can seem immensely time-consuming and expensive. Many businesses, in fact, avoid auditing altogether; they choose to react to situations as they occur and face the consequences at that time.

While undoubtedly an enormous task, electronic data auditing and proactive strategies are possible and manageable. Automation, by far, is the easiest and most cost-effective means to protect your intellectual property. Automation offers

a scalable solution, rarely escalating in price as organizations grow. And, having an automated system minimizes the burden on employees and managers. More important, these systems require little to no human intervention. This means they can adapt to any organization throughout its life cycle and they are much less susceptible to human error.

Question

How does data auditing help good governance?

Answer

Informed decision making in corporations depends on the integrity of the information available to executives. For corporate leaders to make good decisions for the enterprise and its stakeholders (e.g., investors, customers, employees), information must be accurate and trusted. Today, with employees, customers, partners and other individuals having access to data that were previously available only in highly restricted back-office situations, corporations must monitor this expanded access to ensure that the information remains trustworthy. A company without a means to audit data access may base decisions on erroneous information, create weak governance procedures, and invite business and legal problems.

Independent audit solutions, beyond the reach of a small group of privileged users, can ensure data integrity and contribute to good governance. It can also provide business benefits that extend beyond compliance.

For example, if the proposed data auditing solution complies with internal corporate policies and processes, it can extend the company's adherence to these policies and help ensure that individuals and divisions within the enterprise are operating with the same set of ethical guidelines.

Second, a comprehensive data auditing solution can improve internal business processes by tracking and identifying data changes in areas that may not be relevant to public financial reporting or compliance requirements, but could be important in improving product development or manufacturing or creating significant cost savings that would benefit the company.

Third, information available through audit records can be used to answer *ad hoc* business questions, an important business process that may not be part of regular reporting mechanisms. A data auditing solution can track information and changes to data in the corporate database, historical information that previously would have been lost or very difficult to obtain.

With the independent controls that a data auditing solution offers, corporations have the necessary information to prove that their data are accurate and that only authorized changes have been made. This type of internal detection system provides good data to help assure good governance.

Question

How are enterprises addressing risk management in their new corporate agenda?

Answer

Enterprises are addressing risk management in ways they have never done before. An effective risk management oversight system is one of the most essential business tools to identify and manage risks that potentially threaten a company—risks such as fraud, failed audits, lost customers, damage to brand and reputation, and shareholder lawsuits.

A critical component for a thorough risk management system is data auditing. As discussed earlier, auditing an enterprise's databases can safeguard data integrity and, thus, improve business operations. With more sensitive corporate data being captured and maintained electronically, it is the only means to detect changes in corporate information or learn of unauthorized access that could create legal problems.

Today, executives are insisting, and rightfully so, that their management team develop a risk profile for the company and review it frequently, and that internal auditors and the board audit committee be an integral part of this effort.

Although many think that hackers or breached firewalls are the major threat to data integrity, access to corporate databases by unauthorized employees and errors made by internal users are the real culprits. To combat this internal threat, an enterprise data auditing solution provides a trusted, unimpeachable audit trail that eliminates the back doors to corporate data by auditing direct database access by internal users, including privileged IT users.

Important factors that minimize risk when a corporation implements a data auditing solution are the segregation of duties and the separation of the audit system. This ensures that the people who are charged with maintaining the database are not the same as those who conduct the audit. This can be accomplished by instituting a data auditing solution that can be maintained by a different group of employees, to protect against error or misuse by privileged users.

Question

What types of approaches are generally applied to data auditing?

Answer

In the past, there were two generally applied approaches to data auditing, but these may create potential risks or increase the costs of implementing compliance.

Application modifications change the source code of every application that might be used to access the data of interest. This approach can substantially increase the implementation cost of compliance auditing and reduce confidence in the ability to capture a complete audit trail, creating security vulnerability or risk because of the inability to capture changes to permissions and schema.

Trigger-based collection at the data source is the traditional means to capture data modifications. These triggers, which are special-purpose application logic, are extremely difficult to write correctly. The main concern of IT departments over triggers is the substantial run-time performance overhead. In addition, triggers cannot capture data views or changes to schema and permissions.

Nontrigger tracking at the data source is made possible through audit agents, which are associated with each database server containing important data. These audit agents harvest information about data-related activity, and because they operate at the database server, they capture all relevant data activity, regardless of the application used. Applications need not be modified to accommodate this approach.

The ideal solutions for auditing data activity depend on an effective data capture capability. The best approach minimizes performance overhead while consolidating a complete audit of data access across multiple servers and providing active monitoring and alerting. Enterprise-class database audit software provides the ability to capture a wide range of data-related activity, consolidate and manage this information across multiple servers, review and analyze it in a variety of ways, create reports about the activity at various levels of detail, and send timely notifications about certain kinds of detected activity. Prudent organizations are implementing these solutions to meet today's demanding data auditing requirements.

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

WizSoft®
(516) 393-5841 • info@wizsoft.com

Taking Governance Forward

By Patrick Stachtchenko, CISA, CA

Governance: Worldwide Discussions

Governance has been an issue for millennia. Egyptians, Greeks and Romans set up different power structures and processes for decision making. Many recent events such as the following have put governance questions back in the headlines:

- **The 2008 Olympics in Beijing.** Who decided on Beijing? A private not-for-profit organization, the International Olympic Committee. Why? On what basis? What were the commitments taken? What enforcement powers were set out? Why did many countries boycott the opening ceremonies to express their disapproval?
- **The 2008 US presidential election.** Who decided on who could participate in primaries? Why is it different for each state, for each party? How were delegates and super delegates attributed? Is it fair that Florida and Michigan voters do not have a real say in the designation process? Some states had a winner-takes-all approach and others had a proportional rule, why? In the presidential election itself, what makes it acceptable to have an elected president with fewer votes than his opponent?
- **The 2008 international financial crisis.** Why have US and European Central Banks taken opposite options relative to setting interest rates? In the US, the Federal Reserve Bank's mandate is quite large—it covers both inflation and economic growth, whereas in Europe, the primary objective is to maintain price stability. Which is most appropriate? Who has a say in these institutions?

Similar questions exist relative to the mandate, representation, veto power and type of authority of organizations such as the United Nations, G8, G20, International Criminal Court and nongovernmental agencies and to the mechanisms that need to be in place to deal with issues such as the Kyoto Protocol to reduce carbon dioxide emissions; the potential quick, worldwide spread of pandemics; or the trade discussions of the World Trade Organization.

The current governance principles and structures of these organizations have been subject to criticism and controversy. Are they effective to deal with the new expectations? Do they take into account the current interests and influence of the various stakeholders? Each country, each culture, sees the corresponding benefits and constraints with its own eyes. It is not easy to find the appropriate, acceptable mechanisms to share power. There is no clear consensus as to who should be involved, who should have veto power, what type of authority they should have, etc. This is why governance changes are high on the agenda and appear to be critical in ensuring that current and future expectations be met.

Governance Is a Business Issue

As in other domains, the context has changed in the business world and modifications to the governance structure have come to light.

Originally, the business owner had the most say in decisions in the enterprise. Then, corporate structures were put into place to facilitate decision making, as ownership was spread over millions of shareholders. Boards of directors took over many responsibilities. But with time, the chief executive officer (CEO) ended up having a large say in the composition of the board and, in many instances, ruled and controlled the company and its strategy. The only option for shareholders appeared to be to sell their shares if they were not happy with the performance of a specific organization. Many think that this situation contributed significantly to business demises such as Enron and WorldCom.

Proposals were made to reequilibrate the power structure by giving more power and responsibilities to the board and to specific committees, such as the audit committee, to better deal with internal control and fair financial reporting or the remuneration committee to better deal with the basis for the type and the level of remuneration of the CEO. New legislation was put into place, such as the US Sarbanes-Oxley Act and Basel II. Compliance with these pieces of legislation has taken a lot of attention, energy and cost. But, is there appropriate governance set up and applicable all over the world?

New forms of value creation have also appeared recently with, for example, the advent of the Wiki world, with multiple authors and shared intellectual property. This creates muddled ownership and governance issues. Furthermore, there are new governance expectations relative to transparency, corporate responsibility, power sharing and accountability.

Few universally acceptable, agreed-upon governance systems, if any, seem to have surfaced. This is why governance is still high on the agenda of many enterprises.

Governance of IT Is Critical to Success, Yet Remains a Challenge

Originally, IT was implemented to automate processes of enterprises and enable gains in productivity. For many decades, the CEO relied on the chief information officer (CIO) to set up and execute the IT strategy. Others within the enterprise had little to say—but as IT became more strategic and a critical enabler for business transformation and value creation, and also more risky, new governance issues appeared.

Which stakeholders should have a say in decision making? Who should decide on IT budgets, on priorities between

projects, on performance indicators? How should business govern IT? How should the IT function govern IT to respond to business expectations? Should the CIO's role and profile evolve? Which IT committees should be set up? Who should be part of them? What competencies should they have? What kind of decision-making power, responsibilities and accountabilities should they have? To whom should they report? On what should they report? How should they fit with the other governance structures within the organization? What ensures that IT is aligned with business? These and other similar questions are critical issues for most enterprises. Convincing answers have not come easy. Furthermore, traditional stakeholders often do not have the IT competencies and experience to make sound decisions.

In this context, what is the proper way forward?

The Way Forward: An Integrated Enterprise Governance Approach

If only someone would come forward and put all the pieces of the governance maze together, including governance frameworks, principles, structures, processes, practices, views, activities, relationships, roles and responsibilities, and objectives. And, how does all this fit with management frameworks, principles and structures?

To help respond to the above question, the IT Governance Institute® (ITGI™) led an initiative, Taking Governance Forward, to provide an integrated high-level overview of governance.

Enterprises exist to deliver value to their stakeholders. This is done by handling risk advantageously and using resources responsibly. Speedy direction setting and quick reaction to change are essential—decision making must be shared among many. Therefore, governance comes into play. Successful enterprises implement an overarching system of governance that facilitates the achievement of their desired outcomes, both at the enterprise level and at each level within the enterprise.

In this context, a holistic definition of enterprise governance is proposed:

Governance is the framework, principles, structure, processes and practices to set direction and monitor compliance and performance aligned with the overall purpose and objectives of an enterprise.¹

This definition is completed with high-level answers to the following governance questions.

Who is accountable and responsible for governance? Stakeholders, owners, governing bodies and management are responsible and accountable for governance.

What do they do, and how and where do they do it? They engage in activities (set direction, monitor compliance and performance) in relationship with others and use enablers (frameworks, principles, structures, processes, practices) within the governance view appropriate to them (governance of the enterprise; of an organizational entity within the enterprise such as a business unit, division or function; and of a strategic asset within the enterprise or within an organizational entity).

Why do they do it? They institute governance to create value for their enterprise, determine its risk appetite, optimize its resources and use them responsibly.

In summary, the accountability and stewardship are delegated to a governance body by the owner/stakeholder, expecting it to assume accountability for the activities necessary to meet expectations. In alignment with the overall direction of the enterprise, management executes the appropriate activities within the context of a control framework, balancing performance and compliance in achieving the governance objectives of value creation, risk management and resource optimization.

Each enterprise needs to determine its appropriate overall governance system. To help, it was considered that governance implementation guidance and identifying, positioning, comparing and mapping governance frameworks, principles, structures, processes and practices, currently in use, would be beneficial. As a first step, implementation guidance and an initial mapping of IT governance enablers was initiated by the ITGI's Governance on a Page Working Group; much more work needs to be done and more people need to be involved, before a comprehensive overview of governance can be provided.

The Way Forward: A Collaborative Initiative

ITGI and the task force hope that other organizations will further populate the IT governance space or map other views of governance (e.g., governance of organizational entities, such as the finance or the human resources function, or of critical assets, such as strategic alliances or intellectual capital).

Through a collaborative effort, the relationships, dependencies, frameworks, standards, guidance and organizations within the governance landscape will become more clear—and, consequently, will foster better understanding and practical application of the concepts of governance itself.

Endnote

¹ This definition was taken from the Taking Governance Forward project.

Patrick Stachtchenko, CISA, CA

is a past international president of ISACA. He is a partner at Stachtchenko & Associés, a business consulting firm specializing in governance and performance improvement. Previously, he was responsible for Management Solutions, the management consulting practice of Deloitte France. He was also in charge of the computer audit and risk management and the IT consulting practices of Coopers & Lybrand France. He currently serves on ISACA's Strategy Advisory Group and Governance Advisory Council. This last year, he chaired ITGI's "Governance on a Page" Working Group.

Accounting for Value and Uncertainty in Security Metrics

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

There is a good reason why searching for meaningful security metrics continues despite the abundance of purportedly effective ones: because many traditional approaches just do not measure up. They gauge the functionality and efficiency of preventive security measures. Doing such, they are wrong-headed and frequently lead to inappropriate security decisions.

Instead, the effectiveness of security programs,¹ taking into account value and uncertainty, should be measured. This is a much more difficult challenge because it depends on the measurement of the value of something not happening (i.e., a bad outcome that has been deterred, avoided or prevented). But how can one be certain that bad things are not happening due to the security tools and services in place? Is the lack of bad events a matter of chance? Or, were there unrealistic expectations about the existence of threats and the degree of vulnerability? The reality is that total certainty is not attainable.² However, that does not preclude the need to deploy security.

It is better to make good security decisions based upon less-precise estimates of value and risk than to make poor security decisions supported by precise, though inaccurate, metrics. Consequently, it is postulated that it is better to try to improve how to estimate value loss and uncertainty rather than seek out an increasing number of less meaningful, readily measured metrics. It is important to recognize, however, that the techniques described here are not a panacea and there are challenges in measuring less-tangible characteristics such as value loss and uncertainty. Nevertheless, there has been substantial progress recently in the measurement of the value of intangibles,³ which should serve to enhance the practicality of this approach.

Metrics and Security Metrics

Some of the numerous definitions of the terms “metrics” or “security metrics” must be considered.

In the US National Institute of Standards and Technology (NIST) publication *Security Metrics Guide for Information Technology Systems*,⁴ the word “metrics” is defined as follows:

Metrics are tools designed to facilitate decision making and improve performance and accountability through collection, analysis and reporting of relevant performance-related data. The purpose of measuring performance is to monitor the status of measured activities and facilitate improvement in those activities by applying corrective actions, based on observed measurements.

In the *Corporate Information Security Working Group: Report of the Best Practices and Metrics Teams*,⁵ it is stated that:

Metrics are about transforming policy into action and measuring performance. Visible metric scores provide a positive influence on human behavior by invoking the desire to succeed and compare favorably with one's peers. Metrics report how well policies, processes and controls are functioning, and whether or not desired performance outcomes are being achieved ... [Many] metrics ... measure the status or effectiveness of controls, not the underlying risks the controls are intended to mitigate. Risk measurement involves complex consideration of threat event frequency, probability of attack, exposure from vulnerabilities (mitigated in part by controls), and magnitude of potential loss.

In the *Proceedings of the Workshop on Information Security System Scoring and Ranking*,⁶ the expression “IS*” is used, where IS stands for information security and the asterisk can mean any of the terms: metric, measure, score, rating, rank or assessment result. The resulting definition is as follows:

An IS is a value, selected from a partially ordered set by some assessment process, that represents the IS-related quality of some object of concern. It provides, or is used to create, a description, prediction, or comparison, with some degree of confidence.*

If these definitions are taken as means and goals of a security metrics program, a set of requirements can be established and how well various security-related metrics adhere to such requirements can be determined. While the goals are worthy ones, the means of attaining them using the metrics proposed in these and other documents fall far short and, in many cases, can be grossly misleading.

Perhaps the simplest way in which to differentiate between what are commonly taken for security metrics and those measures that more closely represent actuality is to look at the parallel example of computer applications testing.

An Illustration: Comparing Functionality Testing and Security Testing

For illustrative purposes, the testing of custom-developed or commercial off-the-shelf (COTS) computer applications should be considered. For the most part, traditional functionality testing is aimed at verifying the correctness

of the workings of applications and, to some degree, the efficiency of applications and related operational processes.

Functionality testing generally involves developing a series of scripts representing a comprehensive list of activities and interactions usually between the applications and human beings, but also between and among systems and networks. The scripts are run under specific assumptions as to the operating environment of the application, e.g., configuration of the systems and networks, number and locations of nodes and end points, and number and type of end users. The hoped-for result is some form of “certification” that the applications do what they were specified to do, which is not necessarily the same as doing what the owners or users of the applications wanted or expected.

The purpose of security testing is to determine that end users, whether or not they have misdeeds in mind, cannot compromise applications and data that are created and handled by the applications. Thus, the whole orientation of security testing is very different from functionality and performance testing. Functionality testing is designed to ensure that applications do what they are supposed to do, whereas the purpose of security testing is to check that applications do not do what they are not supposed to do.

To ensure that applications and systems are “bulletproof,” which is really an unattainable ideal but a worthy ultimate goal, one must test every possible activity and combination of activities, tracing through all possible threads and hitting routines contained in the application. It is also important to replicate actual production environments as accurately as possible.⁷ The security tester should try to break the system, as opposed to ensuring functionality. Not only is security testing inherently more difficult to do, it also is orders of magnitude greater in terms of number of cases and

complexity than testing to verify correct functionality. Also, if a single security test scenario is missed during security testing, the entire system might be vulnerable to compromise, whereas not testing a single function usually has far fewer, less-damaging implications.

Back to Security Metrics

As with security testing, so it is with security metrics. The traditional metrics approach is to measure deterministically the functionality and efficiency of various security measures, tools and processes. Thus, “typical” security metrics include measures such as number of systems certified per quarter, average viruses found per day, number of vulnerabilities identified weekly, number of users trained per quarter and so on. These were depicted as insufficient measures in the “Enterprise Security Metrics: Taking a Measure of What Matters” presentation by J.F. Stevens and B. Wilke.⁸ While they proposed other measures, they have many of the same failings as traditional metrics in being partial measures from which the most valuable information is missing.

Perhaps the most obvious deficiency in their presentation is that they refer to “number of” on its own. This gives no indication as to relative importance, nor does it identify in any way that which has been omitted or was missed altogether. At the very least, one should gather “number and percentage of.” But, even then, one needs to know the relative importance, from a security risk perspective, of those items both included and excluded.

As an introduction to the concept, various categories of metrics—what they measure and where they might be deficient—should be considered. These considerations are shown in **figure 1**.

Next, each category should be considered in more detail.

Figure 1—Pros and Cons of Various Categories of Metrics

Category of Metric	What It Says	What It Does Not Say
Existence	This type of metric is recognized by its being acquired by means of a question such as “Do you have a patch management program?” for which allowable answers are “yes” and “no” and sometimes “not applicable” and “not known.” It is an indicator of whether something exists.	The problem with this type of metric is that, even if the answer is “yes,” it does not tell the quality, age, accuracy or completeness of the object of the question, unless it also includes a request to see the object. Even then, the assessment may be suspect.
Ordinal	Often, it is not possible to measure something numerically. For example, in answer to a question such as “What is the likelihood that an exploit against a particular vulnerability will be developed and released?,” one might respond subjectively with a view of the probability, loss, etc., as high, moderate or low.	An ordinal measure is usually subjective and may vary from one person or group to another. There are various voting and consensus techniques that attempt to bring some measure of science to this, but a subjective bias still remains.
Score	In this case, one can apply a numeric value, such as one for low, two for medium and three for high, or score on a continuum on a scale such as one to 10.	This type of measure is just as subjective as an ordinal measure. A problem with this type of measure is that it can be misused to give the appearance of high precision. This is because when the scores are tallied and then averaged, a fractional value, which can be shown with a long decimal extension, is obtained. One might assume that this is suggestive of precision, but it is not.
Number (Cardinal)	When asked for a number, such as “How many systems were patched last month?,” the responses can be looked at over time and trends can be indicated. Usually, there are implied values to the number and whether it is increasing or decreasing. Thus, if the number of patched systems increases over time, that might be considered good but it may not represent an improvement if, for example, the number of vulnerable systems is increasing faster than those being patched.	There is no indication with a pure number as to the size or state of the overall population. If, for example, the number of patches is increasing at a lower frequency than the number of exploits, it may represent a situation of increasing risk of loss. However, in such a situation, it is usually safe to say that the number of patches increasing is better than it being level or decreasing, unless, of course, the number of vulnerabilities is realistically decreasing.

(continued on p. 26)

Figure 1—Pros and Cons of Various Categories of Metrics (cont.)

Category of Metric	What It Says	What It Does Not Say
Percentage	<p>Here the question is of the nature: “What percentage of systems was patched last month?” That is clearly more informative than the metric resulting from the previous question, since it indicates whether the relative proportion of patched systems to unpatched systems is growing or decreasing.</p> <p>By making the additional effort to include as many instances of a particular vulnerability as possible, one can make percentages more meaningful and realistic.</p>	<p>Pure percentages do not account for the relative criticality, importance or risk exposure of the systems involved. There is potentially a huge difference in meaning if highly critical systems are among those not patched vs. having only systems of lesser importance not patched.</p> <p>Another important aspect of this is that, while the numerator is generally measurable with a high degree of accuracy, the denominator may not be. For example, while there is a good chance that a good record of the number of systems that have been patched exists, there may not be a good inventory of systems that require a particular patch. This is especially true if systems with the vulnerability are subsumed under other applications, such as happened with the Structured Query Language (SQL) Slammer worm. It came as a surprise to many technology and security staff to learn that a number of common applications had SQL embedded and consequently were taken down by the attack.</p>
Holistic	An even more complete view can be gained by adding known vulnerabilities for which no patches are available.	The issue here is to find a comprehensive and accurate source, since this measure is only as good as the source. There are still known vulnerabilities that are not reported, where the discoverer may have sold the information to a security firm or government agency, for example, and has agreed not to share knowledge of the vulnerability with others.
Value	A better measure of the value of patching may be obtained by determining, albeit in gross terms, the value loss incurred when a vulnerability might be exploited, and calculating the total net loss avoided through the patching program.	While value loss is a more meaningful measure of the effectiveness of a patching program, such estimates are very rough. The results will provide a relative view of various approaches to patching and to specific choices; as to what should be patched and in what sequence, they are still highly subjective.
Uncertainty	The stochastic or probabilistic aspect of patching should be included. After all, when a threat is announced, there will be an estimated time before an exploit appears, and then another variable period before the exploit reaches a particular facility. Such variability can be expressed as probability distributions.	The specification of the probability distributions is also highly subjective. However such probability distributions may be much more representative than point estimates and, therefore, should be considered.

Existence Metrics

There are a number of security tools and practices that comprise a minimum set for any going concern. Such requirements, which are virtually mandatory, typically include antivirus software, firewalls, and written security policy and standards. While knowing that, for example, antivirus software is in place may be somewhat reassuring, it does not guarantee that it has been installed properly and is up to date. However, if any of these items has not been implemented, then one has a clear indication that the organization’s security posture is deficient.

That is to say, while a “no” answer is a clear pointer that action needs to be taken by the respondent, a “yes” answer usually means that further information should be sought. A “not applicable” response might invite verification and a “do not know” reply typically will raise suspicions.

In summary, existence metrics are useful to the extent that they can provide high-level indications as to the security posture of an entity.⁹ Often start-ups lack many fundamental security tools and procedures and, as such, are highly susceptible to security breaches.

Wanting to measure threats to a particular information asset and operational and technical vulnerabilities that might expose an asset to threats is an example of the existence approach. Such an approach is described in the OCTAVESM

method for risk management developed by the Software Engineering Institute at Carnegie Mellon University and described in *Managing Information Security Risks*.¹⁰ Under the OCTAVE approach, various groups within an enterprise complete a series of surveys. The required responses are “yes,” “no” and “do not know”—typical existence metrics. The analysts note the percentages of responses falling into each response category.

Ordinal Metrics

There are many situations in which a numeric value cannot be ascertained and yet just knowing whether or not a particular security tool or procedure exists is insufficient. In such cases, it might be possible to get someone to attach an ordinal value, such as “high,” “medium” or “low,” to the response. The key here is that a person is attaching values to the ordinals so that the assessment of the security tool is very subjective and, more than likely, will vary from one person to another. A further issue with ordinal metrics is that they are not additive (or multiplicative), and they cannot be aggregated or averaged as would numbers or percentages. For example, how would one add a “high” to a “medium” and what would be the result? Would a “high” and a “low” average out to a medium? What if they were weighed differently, with the “high” being three times more significant with respect to exposure than the “low”?

Score Metrics

The obvious answer to the previous question is to attach numbers to the classes of ordinals, for example, applying the score of three to “high,” two to “medium” and one to “low.” To their credit, the creators of the OCTAVE method do not succumb to the assignment of numerical values to quantitative data.

A qualitative approach indicates only relative priority. If you assign numbers to those qualitative measures and then perform mathematical operations on the numbers, you are implying a quantitative relationship that you have not established ... because we have looked only at relative ranking of impact and probability, we can merely conclude that we consider the first risk greater than the second. We cannot begin to say how much greater.¹¹

For example, the results of the BITS Operational Risk Management and Security and Risk Assessment Working Groups that produced a set of key risk indicators (KRIs), which applied numeric values to ordinal results,¹² do an excellent job of laying out threats and vulnerabilities. A great deal of time was spent on what the number ranges should be and how they should be aggregated and reported.

While the use of somewhat arbitrary scores can be questionable, in defense of such an approach, one should accept that because there are so many who subscribe to the “measure to manage” philosophy and who believe that high-precision numeric values are key, there is great pressure to come up with a number. If doing so means the difference between someone using the KRI approach, for example, vs. “shooting from the hip,” perhaps it makes sense to develop such metrics. However, one must remain wary of such an approach and seek more meaningful analyses.

Number (Cardinal) Metrics

Perhaps the most ubiquitous metric of all is the plain number, such as the number of patches applied in the prior month. There is a strong desire by practitioners and their management to come up with and present numeric values, especially as they can be shown as trends and/or compared to other areas, enterprises or industries.

Of course, an important characteristic of numbers is that they are more useful if presented in context rather than in isolation. However, even when context is given, numbers do not necessarily provide sufficient information to be of much value. Thus, with the number of patches, one would want to know how many were critical in nature vs. how many were marginally beneficial, to what platforms the patches were and were not applied, and the total number of available patches. The last item could be presented by providing both the absolute number of patches applied and the total number available, or the percentage of patches applied to the total number available for application.

Even when a number, such as the high temperature for the day, provides an exact measure that is meaningful on its own,

additional contextual information is often sought, such as record high and record low temperatures for that day. These latter numbers are frequently used to interpret trends, for example.

Percentage Metrics

It has been established that a percentage can provide somewhat more information than a pure number. For example, if 100 percent of machines are reported patched, the task is complete; whereas if the report says that, for example, 235 machines were patched, it is unknown whether that is good or bad unless the total population is known. If zero percent are patched, it will most likely make a difference if the population is large or small—or zero!

However, percentages, like numbers, have somewhat limited value in isolation. For example, if it is reported that 79 percent of machines have been patched, the obvious next question addresses either the number of machines patched or the total population of machines.

Holistic Metrics

The goal of a particular metric may not be met if the scope of the environment in which it is measured is restricted. That is, the metric itself may extend to only the boundaries of an enterprise and not beyond. Or, if the scope expands to certain external areas of context, such as the industry, region or sector, it might not cover other important areas relevant to the statistic.

For example, the fact that an enterprise applies a certain patch to 95 percent of machines within one week does not indicate necessarily whether the performance is good or bad. If comparable companies within a sector patched only 50 percent of their machines, then the 95 percent looks good; whereas if every other company has patched at the 100 percent level, then 95 percent is a poor performance. Then again, who is to say that the industry standard is a reasonable one in any particular situation?

As this shows, the narrow view can be misleading and detrimental to an effective security program, while a broader, holistic view might add considerably to the usefulness of a metric. Whether the added value is realized depends heavily on how accurate and relevant the external data might be and what cost and effort are required to obtain them at the desired frequency.

There are a number of sources of external data. Perhaps the most quoted is the annual Computer Security Institute (CSI) survey, formerly known as the CSI/Federal Bureau of Investigation (FBI) survey.¹³ It gives, for a specific sample, the trends in threats and measures applied, for example. There is a question as to whether such statistics are representative and can be applied to any specific internal situation. Sometimes it is advisable to omit such external data rather than include them if their inclusion may be misleading. That is a matter of judgment.

Value Loss Metrics

In essence, the purpose of any information security program is to avoid or reduce costs that might be incurred were a security breach to take place. Here the cost of the

*The narrow view can be
misleading and detrimental.*

security program can be determined usually with a fair degree of accuracy. The issue that needs to be addressed is the estimation of the program benefits. The benefits generally result from the deterrence, avoidance or prevention of security incidents. Benefits are usually expressed in terms of costs avoided, such as the more readily discernable costs of notification, credit bureau services and legal fees. However, they should also include less easily determined costs relating to impact on reputation, such as the loss of customers and employees and the opportunity costs of unrealized potential customers and their business. Also to be considered is the potential loss in stock value affecting shareholders and other stakeholders, as well as the negative impact on company valuation in a takeover situation.¹⁴

That being said, one must recognize that both the tangible costs of customer service, for example, and the intangible costs related to reputation are difficult to predict. For example, it might be known to cost US \$10 per notification letter, US \$20 per year per affected customer to provide credit checking services, and US \$25 each to reissue credit cards (these are all rough numbers, though measurable); however, one still needs to try to predict the number of customers expected to be affected by an incident as well as the probability of such an incident occurring within a given period of time. When it comes to reputation loss, besides the uncertainty regarding the number and timing of events, it is particularly difficult to try to anticipate the number of customers who might end their relationship with the enterprise. Also, it is virtually impossible to estimate how many potential customers did not sign up because of privacy concerns.

Accounting for Uncertainty

As described previously, there can be many difficulties in trying to estimate the cost avoidance numbers of a security program because of the high degree of uncertainty as to the value losses incurred due to an incident. However, there are uncertainty aspects relating to all security metrics, even those that initially appear to be cut and dried. For example, as mentioned previously, when calculating the percentage of vulnerable machines that have been patched, one cannot be absolutely certain that all relevant machines have been addressed due to the potential for missing vulnerabilities' embedded systems. Additionally, when evaluating the overall patching program, one might derive performance metrics for known vulnerabilities, with and without available patches, but may never know how many other vulnerabilities have been discovered, but not publicized and, therefore, not patched. Similarly, as has been described, there is uncertainty in the timing of the creation and release of exploits.

The bottom line is that, despite the appearance of certainty and accuracy in many metrics, even the most deterministic of metrics may have probabilistic aspects and there are many proposed metrics that are steeped in uncertainty. Does that mean, as some suggest, that they are not true metrics since, at the very least, they may not be repeatable? Uncertainty does not eradicate necessarily the usefulness of a metric, and the inclusion of probabilistic or stochastic analysis is not only beneficial, but mandatory. Furthermore, there are good foundations to the methods of decision making under uncertainty, which can be exploited.

Conclusions

The definition and measurement of security metrics have been officially recognized as "hard problems" in a report by the INFOSEC Research Council (IRC).¹⁵ But hard problems can be solved, albeit often with considerable effort. This article points out specific deficiencies in current popular metrics and advises that analysts be circumspect in their use.

That is not to say that there is no value in today's metrics—because there is. Unfortunately, the rule appears to be that measurability and usefulness are in contention when it comes to security metrics. However, readily available metrics can be used, if they are used with an appropriate level of thoughtfulness and understanding. At the same time, continued advancements must be pushed to introduce more meaningful, if less easily determined, security metrics.

Endnotes

- ¹ In a presentation dated April 2005, titled "Enterprise Security Metrics: Taking a Measure of What Matters" by J. F. Stevens and B. Wilke of the Software Engineering Institute of Carnegie Mellon University, the presenters claim to have replaced traditional and inadequate security metrics with "enterprise security metrics." The latter are supposed to measure the effectiveness of security programs. They may be better than prior attempts, but suffer many of the same deficiencies of other measures. The presentation was retrieved on 27 May 2007 from a web site but is no longer available.
- ² There are many examples, including: Was Y2K (the millennium date rollover) relatively uneventful because of the huge remediation effort or because the risk was overblown by those wishing to profit from it? Have the efforts of the US Department of Homeland Security prevented another terrorist event in the US like those of 11 September 2001 or have the terrorists not attempted a major attack? Is global warming due to carbon emissions, a natural cycle or both? Will reducing emissions make a significant difference?
- ³ Hubbard, D. W.; *How to Measure Anything: Finding the Value of Intangibles in Business*, John Wiley & Sons, USA, 2007
- ⁴ Swanson, M.; N. Bartol; J. Sabato; J. Hash; L. Graffo; *Security Metrics Guide for Information Technology Systems*, NIST Special Publication 800-55, National Institute of Standards and Technology, USA, July 2005, p. 9, <http://csrc.nist.gov/publications/nistpubs/800-55/sp800-55.pdf>
- ⁵ Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census, Government Reform Committee, *Corporate Information Security Working Group: Report of the Best Practices and Metrics Teams*, US House of Representatives, USA, 10 January 2005, p. 5, www.educase.edu/ir/library/pdf/CSD3661.pdf
- ⁶ Computer Security Associates, *Proceedings of the Workshop on Information Security System Scoring and Ranking*, May 2001, p. vii, www.acsac.org/measurement/proceedings/wissr1-proceedings.pdf

⁷ The author knows of one particular case in which a system had been tested thoroughly “in the lab,” only to fail repeatedly and intermittently in live production mode. It turned out that the high quality of the installation of the laboratory meant that certain failure and recovery routines, which would normally be invoked under certain error conditions, were never tested, since the program had never had occasion to call on them. When installed in a production environment, with less-than-optimal cabling, the program detected transmission errors and branched to the error routines, as it was supposed to do. These error routines failed and brought down the system.

⁸ *Op cit*, Stevens

⁹ *Op cit*, Hubbard, p. 23, refers to this category more generally as “nominal measurements,” which are “set membership” statements.

¹⁰ Alberts, C.; A. Dorofee; *Managing Information Security Risks: The OCTAVESM Approach*, Addison Wesley Professional, USA, 2002, p. 12-13

¹¹ *Ibid.*, p. 224

¹² BITS, *Kalculator: BITS Key Risk Measurement Tool for Information Security Operational Risks*, USA, July 2004, www.bitsinfo.org/downloads/Publications%20Page/BITS%20Calculator/bitaskalnarrative.pdf

¹³ Computer Security Institute, *CSI Computer Crime and Security Survey*, October 2007, www.gocsi.com/forms/csi_survey.jhtml (registration required)

¹⁴ Attempts to demonstrate that stock prices are negatively impacted by the announcement of a security breach have had variable results, with stock prices actually going up in some circumstances. However, the impact of a breach may well be overshadowed by other factors, such as positive current earnings, an overall bullish market, and so on. Also, even if the stock price does rise, it may have gone up even more had the breach not occurred.

¹⁵ INFOSEC Research Council (IRC), “Hard Problem List,” November 2005, www.infosec-research.org/docs_public/20051130-IRC-HPL-FINAL.pdf

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

is the business information security officer and chief privacy officer for U.S. Trust, Bank of America Private Wealth Management, where he assesses and mitigates privacy and security risks through awareness programs and the enforcement of system access controls. He is currently a member of the Financial Services Sector Coordinating Council (FSSCC) Research and Development Committee, and was honored with the Information Security Executive (ISE) Luminary Leadership Award in 2007 and the *ComputerWorld* Premier 100 IT Leaders Award in 2003. Axelrod is the author of the book *Outsourcing Information Security* and a chapter on return on security investment in *Managing Information Assurance in Financial Services*.

HighPoint Audits **HighPoint Assessments**

The Next Generation GRC Solution

HighPoint Controls **HighPoint Policies**

HighPoint Enterprise from Favored Solutions

A new breed of browser-based software addressing the management of Governance, Risk and Compliance

Favored Solutions
1-832-261-4747
www.favoredsolutions.net

Harness the power of the full suite or leverage the robust functionality of a single module. It's your choice.

- Internal Audit Management
- Risk Assessments and Analytics
- Enterprise Risk Management
- Internal Controls Management
- IT Governance
- Policies and Procedures
- Workflow Powered
- Executive Reporting and Dashboards

INDUSTRY LEADER
The Institute of Internal Auditors

Username: ITGovernanceSuperstar
Password: SMU-ISACA

SMU. The world's first engineering school to partner with ISACA.

SMU's Master of Science in Information Engineering offers courses that meet ISACA's internationally recognized curriculum. Future CIOs can master the foremost management elements of a global IT operation. Information Engineers and IT Security Professionals learn to design high-integrity systems. And IT Auditors can gain one-year work experience toward a Certified Information Systems Auditor certification. It's a highly respected career choice for the highly motivated.

For more, visit EngineeringLeaders.smu.edu or phone 214-768-2002.

SMU ENGINEERING

Southern Methodist University will not discriminate in any employment practice, education program, or educational activity on the basis of race, color, religion, national origin, sex, age, disability, or veteran status. SMU's commitment to equal opportunity includes nondiscrimination on the basis of sexual orientation.

Implementing, Automating and Validating Controls for Privileged Users in Healthcare Organizations

By Cheryl Traverse

A recent Insider Threat Study by CERT found that 86 percent of insider attacks in enterprises originated from people who are or were previously full-time employees in a technical position within the enterprise.¹ Insiders typically have access to privileged data beyond their authorization and are far more capable of exploiting loopholes in a network than outsiders.

A 2006 US Department of Justice study determined that the average loss per incident was US \$1.5 million.² In a healthcare enterprise, however, these costs would also include those associated with the loss and compromise of private medical data. Therefore, it makes sense that the implementation, automation and validation of controls for privileged users are requirements for healthcare companies to satisfy stringent compliance standards such as the Health Insurance Portability and Accountability Act (HIPAA) and the Sarbanes-Oxley Act.

This is a particularly difficult challenge for healthcare companies for two reasons. First, these companies are usually large, global enterprises with traditional and complex heterogeneous infrastructures. These infrastructures include a mixture of standard IT devices and systems and nonstandard equipment in the form of medical devices, which pose unique security challenges. Second, the healthcare internal user group (including IT operations personnel, outsourced technical employees, application developers and vendors), members of which all work within the critical infrastructure, is particularly hard to control due to its high level of skill and regular use of powerful access tools.

Medical Device Service and Maintenance Visibility Gaps in Healthcare

A medical treatment facility contains technologies and systems (such as CT scanners, patient monitoring devices and test equipment) that are outside the realm of conventional IT infrastructure components, are generally beyond the scope of standard IT security measures and often leave holes vulnerable to security breaches. Such facilities may have dozens of pieces of medical equipment from various manufacturers, supported remotely. Typically, the equipment vendors require a virtual private network (VPN) connection to the facility's network to support their equipment. While this practice is common, it introduces unnecessary security risks by exposing sensitive data to outside parties who may not have security as a top priority. Even segregating these network-enabled medical devices from the IT infrastructure

network does not eliminate patient data breaches, simply because many approved (by, for example, the US Food and Drug Administration) medical devices operate using legacy technology.

Merging IT Operations and Medical Device Service and Maintenance Platforms

Traditionally, medical device service/maintenance differs from standard IT operations in that medical devices utilize serial communication as the primary transport, while IT operations utilize the network (TCP/IP) transport. However, all other things being equal, the process of upgrading, troubleshooting, transferring data and performing other tasks on a medical device is fundamentally the same as it is with an application server or a network infrastructure device. Consequently, because most medical devices are now manufactured with built-in network transport capability, servicing a medical device is almost identical to servicing an IT infrastructure component. Treating the service of medical devices like the service of an application server lets IT have a better focus on security best practices and minimizes the impacts of legacy technology.

IT Operations Visibility Gaps in Healthcare

In most healthcare enterprises, testing and monitoring of IT resources—networks, servers, applications and databases—are done using well-established best practices. With security levels heightening, many enterprises also routinely test and monitor their perimeter security systems with firewall penetration tests, intrusion detection/prevention and virus filtering.

However, even with these measures in place, the question still remains: how do these enterprises address the threats to security and compliance presented by partners, vendors, offshore developers, managed service providers, internal IT operations, and other privileged and external users that have been admitted to the network? Is there an effective method of implementing, automating and, finally, validating controls for high-risk users that closes visibility gaps and ensures compliance?

Many benefits can be achieved through the consolidation of device service/maintenance and IT operations, but healthcare enterprises must take into consideration some guidelines for using consolidation to implement and validate controls.

Guidelines for Implementing and Validating Controls

Guidelines for implementing and validating controls follow.

Know the Access Model

With a VPN connection, which is required by most vendors, the access model typically features a predefined encrypted domain and a default access policy. Regardless of whether it is a Secure Sockets Layer (SSL) or IP Security (IPSec) protocol, the access model gives a VPN user full access to all the resources inside that encrypted domain. To require particular VPN users to reduce their access to authorized resources, exceptions in the form of rules or nested access policies must be created to block the user from all unauthorized resources within the encrypted domain. The enterprise must be aware of its current access model and take steps to create more secure policies.

In evaluating security measures that are more robust than the typical VPN model, healthcare enterprises should consider adopting technology that allows them to adhere to the “principle of the least privileged,” also known as “deny all, permit by exception” (DAPE). In the DAPE model, each user or group account starts with no access or visibility to anything in the infrastructure. To grant users access to specific resources on the network, an exception is created to give highly granular resource access permission to an individual user or group of users, allowing visibility to only that explicit resource.

In this way, switching from a VPN model to a DAPE model provides an immediate security improvement. Moreover, the DAPE model simplifies testing and monitoring of access policy control, because no privileged users have access by default and each is granted access to only a short list of specifically authorized resources. This condition is much easier to test and monitor than if these users had full access by default and each had to have a long list of rules blocking out unauthorized resource access.

Separation of Duties Through Compartmentalization

The biggest challenge many enterprises face is not how to let users into the network, but how to ensure that they are given visibility only to explicitly authorized resources, so that critical information, such as patient data and classified content, is not compromised. Many healthcare firms are seeing an increased need for sharing data across separate untrusted domains, which exposes private data to a number of security vulnerabilities as they make their way across the network. For example, medical information from US servicemen and women in the field is shared among any number of systems belonging to the US Department of Veterans Affairs and the Department of Defense. Compartmentalization is the key to achieving true segregation of duties, as required by many regulations for sharing resources across unsecured domains.

Techniques such as port-based access provisioning provide highly granular control regarding what the authorized user can see, while hiding everything else. For example, utilizing a port-based access method, a healthcare enterprise can let a vendor in to troubleshoot a database, but can also prevent that external user from reaching the operating system on which the database server is running.

Eliminating unnecessary exposure to the IT infrastructure and limiting individual users’ reach when they are on the

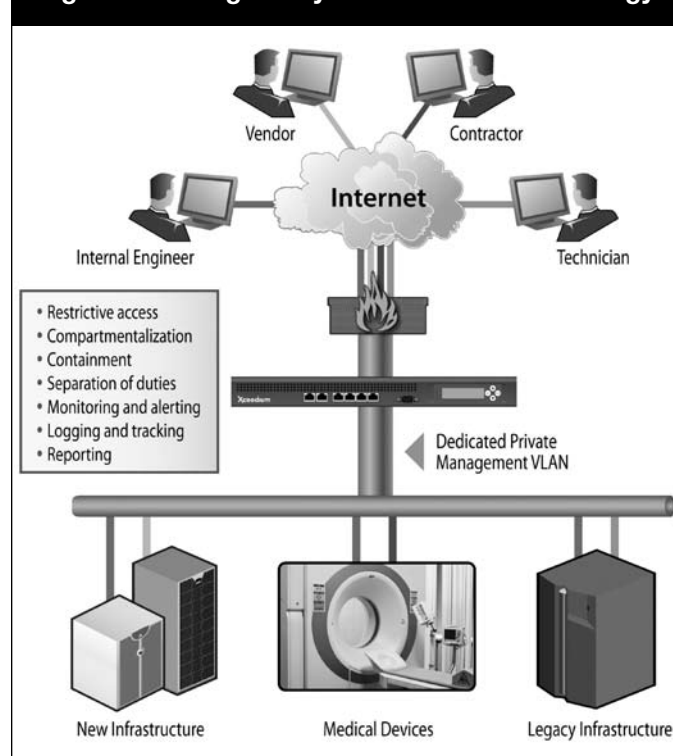
network effectively reduce the scope of implementation and validation of controls, which, in turn, reduces the overall cost of compliance.

Containment to Authorized Access Areas

The biggest source of exposure for healthcare enterprises derives from “leapfrogging,” or the ability of an admitted user on the network to hop from an authorized resource to other, unauthorized resources on the same network. The lack of access containment security controls, and subsequent leapfrogging, is the biggest vulnerability for any healthcare organization that grants remote access to privileged and external users.

Many healthcare companies have no trouble developing security policies to prevent leapfrogging, but find that implementation and enforcement of those policies is very difficult. One way to do so is by using policy enforcement technology that effectively contains users to their respective authorized areas by automatically monitoring and testing changing conditions to detect any user attempts to jump to an unauthorized server or device on the network (see **figure 1**). Security policy enforcement technology can be a very useful tool for any healthcare enterprise looking to streamline the implementation and validation of controls. Enforcement technology has progressed significantly in recent years, and should be considered when developing a healthcare company’s security plan.

Figure 1—Using Policy Enforcement Technology



Tracking and Reporting of User Activities

Centralized tracking and logging of user activities are essential to passing the audits necessary to achieve regulatory compliance. As such, healthcare enterprises should consider implementing session recording for both command-line

interfaces (CLI) and graphical applications. These can provide the forensic details necessary to support the results obtained from routine monitoring and control tests, as required by the compliance department or the external auditors for the healthcare enterprise.

Centralized Reporting for Testing of Controls

HIPAA regulatory compliance mandates are weighing heavily on virtually all areas of the healthcare industry. While healthcare companies are aware of the criticality of testing controls, particularly for third-party privileged users, many are not doing so because the task is daunting, time-consuming and incredibly resource-intensive. Centralizing all monitoring and tracking in one platform allows enterprises to easily deliver testing of controls for third-party privileged users. This centralization can also be extended to feed information to existing security information management (SIM)/security event management (SEM) systems.

It is imperative that healthcare enterprises carefully examine their current security policies to determine whether they are effectively addressing insider threats. With the availability of infrastructure security technologies that provide automation and validation of controls at never-before-seen levels, it is more viable than ever for healthcare companies to unobtrusively and cost-effectively protect the critical network and meet mandatory compliance requirements.


Endnote

¹ Moore, Andrew P.; Dawn M. Cappelli; Randall F. Trzeciak; *The Big Picture of Insider IT Sabotage Across US Critical Infrastructures*, CERT Program, May 2008, www.cert.org/insider_threat/

² Bosen, Bill; "Network Attacks: Analysis of Department of Justice Prosecutions 1999-2006," Trusted Strategies LLC, August 2006

Cheryl Traverse

is president and chief executive officer (CEO) of Xceedium. She has set the strategic direction, built revenue traction and sold five companies in the past 12 years. She has been a president/CEO of companies in the web authoring, personalization and merchandising application, integration, mobile middleware platform, and Linux application security space. Traverse sits on the advisory board and mentoring forum of the Women's Technology Cluster, on the advisory board of the Forum for Women Entrepreneurs, and on the board of the San Francisco League of Women Voters. She was awarded the TrailBlazer Award in 2002 and the LodeStar Award in 2003 from Forum for Women Entrepreneurs.




Is data the weak link in your IT program?

Our Data Governance Team can assess your data management practices for benchmarking & improvement.

Data Management Practices Assessment (DMPA)

For information including scientifically-validated results, contact
804.521.4056 · dmpa@datablueprint.com · datablueprint.com



ExamMatrix Smarter, Faster

CISA Exam Review

Authored by SRV's S. Rao Vallabhaneni

- 1,700 Multiple Choice Questions
- Greatly Reduced Study Time
- Pass or Refund Guarantee
- No Lock-Out

www.ExamMatrix.com/ISJ
1.800.272.PASS

EXAMMATRIX™

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. 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 and Illegal Acts Effective 1 September 2008
- G10 Audit Sampling Effective 1 August 2008
- G11 Effect of Pervasive IS Controls Effective 1 August 2008
- G12 Organisational Relationship and Independence Effective 1 August 2008
- G13 Use of Risk Assessment in Audit Planning Effective 1 August 2008
- 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
- 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
- G40 Review of Security Management Practices Effective 1 December 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 1999510 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

www.isaca.org/standards

ISACA 2008-2009 Standards Board

- Chair, Ravi Muthukrishnan, CISA, CISM, FCA, ISCA, Capco IT Service India Pte. Ltd. Netik LLC, India
- Shawn Chaput, CISA, CISM, CISSP, PMP, Canada
- Maria Gonzalez, CISA, CISM, Department of Defense, 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
- Edward Pelcher, CISA, Office of the Auditor General of South Africa, South Africa
- Jason Thompson, CISA, CIA, CISSP, KMPG LLP, USA
- Meera Venkatesh, CISA, CISM, ACS, CISSP, CWA, Microsoft Corp., USA

Prepare for the 2009 CISA Exams

ORDER NOW—2009 CISA® Review Materials for Exam Preparation and Professional Development

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

CISA Review Manual 2009

ISACA

The *CISA® Review Manual 2009* 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 information systems (IS) auditors and the knowledge required to plan, manage and perform IS audits. The Study Guides edition also features new content based on the *IT Assurance Framework™ (ITAF™)*, recently published by ISACA. ITAF is a comprehensive assurance model that incorporates standards and good practices, providing guidance on the design, conduct and reporting of IT audit and assurance assignments; defines terms and concepts specific to IT assurance; and establishes standards that address IT audit and assurance professional roles and responsibilities, knowledge and skills, diligence, conduct, and reporting requirements. The *CISA Review Manual 2009* also includes brief chapter summaries focused on the main topics and new case studies to assist a candidate in understanding 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. 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 2009 edition has been developed and is organized to help prepare the CISA candidate in understanding the essential concepts and studying the following job practice areas:

- IS audit process
- IT governance
- Systems and infrastructure life cycle management
- IT service delivery and support
- Protection of information assets
- Business continuity and disaster recovery

CRM-9 English Edition
CRM-9F French Edition
CRM-9I Italian Edition
CRM-9J Japanese Edition
CRM-9S 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 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 2009*.

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

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

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

CISA Review Questions, Answers & Explanations Manual 2008 and 2009 Supplements

ISACA

Developed each year, the *CISA® Review Questions, Answers & Explanations Manual 2009 Supplement* and *2008 Supplement* are recommended for use when preparing for the 2009 CISA exam. Each edition consists of 100 sample questions, answers and explanations based on the current CISA job practice areas, using a process for item development similar to the process for developing actual exam items. The questions are intended to provide 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.

2009 Editions

QAE-9ES English Edition
QAE-9FS French Edition
QAE-9IS Italian Edition
QAE-9JS Japanese Edition
QAE-9SS Spanish Edition

2008 Editions

QAE-8ES English Edition
QAE-8FS French Edition
QAE-8IS Italian Edition
QAE-8JS Japanese Edition
QAE-8SS Spanish Edition

CISA Practice Question Database v9

ISACA

The *CISA® Practice Question Database v9* combines the *CISA Review Questions, Answers & Explanations Manual 2008* with the *CISA Review Questions, Answers & Explanations Manual 2008 Supplement* and *2009 Supplement* into one comprehensive 800-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 2009*. 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 80 MB of available space
- CD-ROM drive
- Display with recommended resolution of 1024 x 768

CDB-9 English Edition—CD-ROM
CDB-9W English Edition—Web site download
CDB-9S Spanish Edition—CD-ROM
CDB-9SW Spanish Edition—Web site download

CISA Online Review Course

ISACA

A complete web-based exam review course is available at www.isaca.org/elearningcampus.

To order CISA review materials for the June/December 2009 exams, see the order form on page S-8 in this Journal or visit www.isaca.org/cisabooks.

Is the IT Risk Worth a Control?

Defining a Cost-value Proposition Paradigm for Managing IT Risks

By Sudhakar Sathiyamurthy, ITIL, MCSE

Nothing puzzles an enterprise's technology officer or an IT controller like the term "cost-value" when deciding investments made in IT risk management. Today, business is more tactical; the decision makers examine the value proposition toward controlling the enterprise's IT risk. The conventional approach to managing IT risks is to look out for a change in the current business scenario, i.e., a paradigm shift from vague decision-making techniques to a data-driven pragmatic approach.

The forthcoming methodology provides a comprehensive outlook for an enterprise to manage its IT risks through a data-driven approach. The background behind the development of this approach is to arrive at a standardized methodology for an enterprise that strikes a correct balance between the cost and value elements of managing its IT risks, eliminating any disproportionate expenditure on the solutions/controls. The approach has been architected in alignment with enterprise risk management (ERM) concepts, industry best practices and the data-driven techniques that have evolved over the author's years of consulting with diverse clients.

This article is structured in two major sections, the risk analysis stage and the control selection stage; each stage is broken down further into substages. A scenario walk-through is provided at the end of each stage, to provide practical insight to the approach.

Figure 1 illustrates the risk analysis and control selection stages and their corresponding substages.

Risk Analysis Stage

The risk analysis stage includes the following substages.

Explore Threats and Vulnerabilities

These stages explore the threats and vulnerabilities of the systems, spread across the inspection universe, through a thorough analysis of the inherent and the interdependent threat sources. The methodology is as follows:

- **Establish inspection universe**—The inspection universe refers to the systems and the interdependencies that fall under the scope of the risk analysis exercise.
- **Discover environmental dependencies**—The overall consolidation of IT infrastructure has been accompanied by increasing technical linkages and interdependence within and across businesses. This phase is intended to identify all possible interdependent threat sources, through clear examination of environmental dependencies of the system under scope. Environmental dependencies refer to the handshake/communication points of the system under scope with the business, technology and operational environments (i.e., development, test, production).
- **Identify threats and vulnerabilities**—Based on the

Figure 1—Risk Analysis and Control Selection Stages and Substages



inferences derived from the environmental dependencies, this phase analyzes all potential inherent and interdependent threats and vulnerabilities within the inspection universe, by adopting techniques such as manual interpretation, vulnerability scanning and attack simulation.

Evaluate Risk Probability

The evaluation of risk probability involves estimating—through expert judgments, historical event analysis, and by drawing inference from the threat and vulnerability identification stage—the probability of the threat source attacking the system within the inspection universe.

During early stages of the project, the threat and vulnerability identification exercise reveals significant numbers of newly explored threats, and insufficient historical data are available to enable a complete quantitative analysis. In this situation, one may have to strike a balance between qualitative and quantitative analysis, through expert judgments. The methodology is as follows:

- **Classify and categorize risks**—Risk classification is the process of analyzing the threats, discovering related patterns and matches among the threats identified, and classifying the associated patterns into distinct subsets, which are further tagged to a threat clause. Based on the aforesaid classification, one may ascertain that controlling an independent threat clause would pass along the mitigation to all its interrelated subsets. The threat subsets are further reviewed and categorized against two discrete parameters—threats associated with historical events and newly explored

threats—for there are unique approaches to calculating the risk probability and cost at risk, which are described in the subsequent risk analysis stages.

- **Calculate risk probability**—Risk probability involves calculating the probability the threat source will attack the system under scope, based on the historical events reported over a sampled time period. Risk probability is calculated as an annual estimate and is expressed in percentage scale. The selection of a sample period requires expert judgment, where reliance has to be placed on factors such as:
 - The sample time frame reporting of a considerable number of risk events required to perform meaningful analysis
 - The sample time frame's lack of witness to a substantial change to the system under study

As said earlier, in the event of newly explored threats, one may have to incorporate logical judgments toward calculation of risk probability, as historical analysis could not be performed. The threat classification and the threat type could provide valuable inputs for making judgments.

For the category of threats associated with historical events, the risk probability is calculated as:

$$\text{Risk Probability} = (\text{Total Number of Risk Events Reported Over a Sampled Period} / \text{Sampled Number of Years}) \times 100$$

Estimate Cost at Risk

The cost at risk substage involves estimating the value of damage that the risk event can impose to the system under scope. A tangible estimation technique, with due consideration of direct, indirect and overhead costs, has to be arrived at by an entity by calculating the cost of the risk event. In the case of newly explored threats, the calculation of the cost at risk requires expert judgment, in close liaison with other key elements such as the service impacted and service commitments. For threats associated with historical events, the cost at risk is calculated using the following methodology:

- **Determine average restoration cost**—The average restoration cost is calculated as the average clean-up costs of all threat subsets associated with the threat clause for the sampled time period. The average restoration cost is calculated as:

$$\text{Average Restoration Cost} = \frac{\text{Sum of the Cleanup Costs}}{\text{Number of Risk Events Reported Over the Sampled Period}}$$
- **Calculate cost at risk**—The cost at risk is the restoration cost calculated for the probable number of risk events identified on the system under study. The calculation should follow a bottom-up approach, whereby the cost at risk, pertaining to the threat subsets, is calculated first, followed by the threat clause. The association of the threat clauses with the systems under study can unveil the cost at risk tagged to the overall system. The cost at risk is calculated as:

$$\text{Cost at Risk} = \text{Risk Probability} \times \text{Average Restoration Cost}$$

Prioritize Risk

Risk prioritization provides a systematic means of prioritizing risks based on the risk exposure rating, which is calculated from the inputs received from the risk probability and the cost at risk stages.

The methodology is as follows:

- **Prepare risk probability score catalog**—The risk probability score catalog integrates a scoring system to the earlier calculated risk probability values, whereby one could ascertain the risk probability levels as critical, medium

and low, with rankings assigned at each level. **Figure 2** illustrates a simple risk probability scoring system.

Figure 2—Simple Risk Probability Scoring System

Risk Probability Range	Levels	Numeric Score
1% to 25%	Low	1
26% to 60%	Medium	2
>60%	Critical	3

- **Prepare cost at risk score catalog**—Similar to the risk probability score catalog, the cost at risk score catalog utilizes a scoring system to define high, medium and low cost at risk levels for the earlier calculated cost at risk values. **Figure 3** illustrates a simple cost at risk scoring system.

Figure 3—A Simple Cost at Risk Scoring System

Cost at Risk Range	Levels	Numeric Score
1% to 25%	Low	1
26% to 60%	Medium	2
>60%	Critical	3

- **Prepare risk exposure score catalog**—The risk exposure score is derived as a product of the risk probability score and the cost at risk score, as follows:

$$\text{Risk Exposure} = \text{Risk Probability} \times \text{Cost at Risk}$$

Figure 4 illustrates the risk exposure scoring system.

Figure 4—The Risk Exposure Scoring System

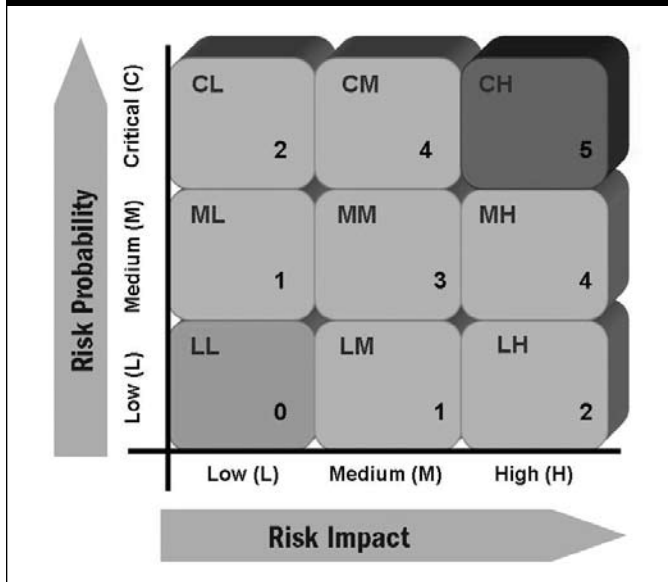
Risk Exposure	Low Cost at Risk (1)	Medium Cost at Risk (2)	High Cost at Risk (3)
Low Probability (1)			
Medium Probability (2)			
Critical Probability (3)			

- **Prepare risk prioritization catalog**—This involves integrating a scoring system to the risk exposure ratings, where the outcome represents the risk prioritization scores and their corresponding priority levels. The risk prioritization matrix provides an insight to the prioritization system. **Figure 5** illustrates the risk prioritization scoring system, and **figure 6** illustrates the risk prioritization matrix.

Figure 5—Risk Prioritization Scoring System

1(LL)	Acceptable	0
2(LM,ML)	Low	1
3(CL,LH)	Medium	2
4(MM)	High	3
6(CM,MH)	Too High	4
9(CH)	Critical	5

Figure 6—Risk Prioritization Matrix



All threat subsets and threat clauses should be rated independently against the scoring system illustrated for risk probability, cost at risk, risk exposure and risk prioritization, to assess the relative significance of each identified threat that contributes to the overall system risk priority. The scoring exercises performed on all threat subsets and threat clauses evolve in their respective catalogs.

The risk prioritization catalog provides the business with an understanding of its current risk exposures and its priorities, which subsequently would help it in controlling risks in an organized fashion.

Example Scenario Walk-through

Multiple events were reported over the last few years on the real-time gross settlement (RTGS) systems of “ABC” financial institution. As a precursor to controlling the risk events, the entity sought assistance from external specialist groups to review its RTGS systems. The inspection universe was established to accommodate systems within the RTGS environment and its interface components. A comprehensive threat and vulnerability analysis was performed on the systems under review and their environmental dependencies. The review system (System X) within the RTGS inspection universe had reported three potential risk events over a sample period of four years. The financial institution had already performed the cost estimation of fixing the risk events, based on the capital, operational and resource expenditures. The cost accrued to fixing event 1, event 2 and event 3 was found to be US \$45,000, US \$39,000 and US \$43,000, respectively.

The risk probability for System X is calculated as $(3/4) \times 100 = 75$ percent.

The average restoration cost for the system is calculated as $(US \$45,000 + US \$39,000 + US \$43,000) / 3 = US \$42,333$.

The annual cost at risk element is calculated as $(US \$42,333 \times 0.75) = US \$31,750$.

By analyzing the risk probability and the cost at risk elements, one could infer that a risk probability level of 75 percent is positioned at critical level in the risk probability scoring system and a cost at risk value of US \$31,750 is rated

at a high-impact level in cost at risk scoring system. The risk exposure score is calculated as critical, based on the risk probability and the cost at risk scores.

Control Selection Stage

The risk analysis stage includes the following substages.

Short List Controls

The short-listing of controls involves planning risk treatment methodologies in controlling the consequences of risk, by mitigating the risk probability.

The methodology is as follows:

- **Identify risk treatment plan**—The risk prioritization exercise aids the business in controlling the analyzed risks through risk treatment plans. Some risks may be considered potentially destructive, in which case an organization may choose to avoid them completely or it may seek to transfer them. Other risks may be accepted with no further actions, depending on the organization’s risk acceptance level.
- **Short list suitable solutions**—The proposed solution might be a single control or a combination of controls, based on the criticality of the risk, where a combination control could be partly preventive and partly detective in nature. In the event that multiple proposed solutions subsist for a particular risk item, the most appropriate ones should be short listed based on cost, adoptability, maintainability and scalability factors.

Evaluate Residual Risk for the Proposed Control

The calculation of residual risk for the proposed control would allow an organization to estimate the overall risk factor that will be mitigated on implementing the said control/solution. If the estimated residual risk level breaches the organization’s risk acceptance threshold, the business could analyze opportunities toward further strengthening the control.

The methodology is as follows:

- **Identify control achieved**—Control achieved is calculated through solution analysis of the short-listed controls. The solution analysis exercise is conducted through an assessment comprised of weighted questionnaires, referencing three key elements: robustness factor, operational effectiveness factor and resilience factor. The score is further translated to a percentage scale, which characterizes the control achieved.
- **Calculate residual risk**—Controls do not always completely eliminate risk. Any risk remaining after implementing a control is referred to as “residual risk.” Though it seems premature to calculate the residual risk before implementing a control, one could estimate the effectiveness of the proposed control by calculating the residual risk based on the previously calculated control achieved value. The logic behind the calculation of residual risk for the proposed control is to identify the amount of control lost on the probable risk element.

Residual risk can be calculated as follows:

$$\text{Residual Risk} = \text{Control Lost} \times \text{Risk Probability}$$

Control lost can be calculated as:

$$\text{Control Lost} = (1 - \% \text{ of Control Achieved})$$

Analyze Cost-value Proposition

The calculation of the cost-value proposition involves evaluation of the cost-benefit of implementing the proposed solution. The value derived out of the calculation provides a data-driven decision system for management to realize the cost-benefit of implementing the proposed control.

The methodology is as follows:

- **Calculate cost at risk (with control)**—The cost at risk calculation with control provides, as an estimated value of damage, what the risk event can impose to the system under scope after the implementation of the proposed control. The estimation utilizes the input derived from the residual risk toward calculation of the cost at risk (with control). Cost at risk (with control) can be calculated as:

Cost at Risk (With Control) = Residual Risk X Average Restoration Cost

- **Calculate cost of control**—The cost of control is defined as the sum of the solution cost and the cost at risk (with control). The rationale behind this logic is, on selecting the said control, the business has to accommodate the solution cost and the cost at risk (with control), since, in most cases, the solution may not control the risk completely and may leave behind some residual risk which, in turn, associates a cost factor to it. If the said solution completely controls the risk without any residue, then the cost at risk (with control) will be zero and the cost of control is equal to the solution cost.

The solution cost must be expressed as an annual spend figure. Any solution has a desired lifetime. (Any major change or upgrade to business might demand a change or upgrade to the solution, too). The solution lifetime value is a judgmental value specific to a business unit, which, in turn, is driven by the organization strategy, core functional domain and more. If the solution lifetime value is n years, then the overall solution cost has to be approximated to an annual value for calculating the cost of control:

Cost of Control = Cost at Risk (With Control) + Solution Cost (Corrected to Annual Spend)

- **Calculate cost-value proposition**—The cost-value proposition is calculated as the difference between the cost at risk (cost at risk without control, calculated as part of the risk analysis stage) and the cost of control. The logic is straightforward. If the outcome of the calculation reveals a positive value, then it is certainly considered cost-effective; if the value is negative, though it is not cost-effective, it needs an expert's judgment to analyze the benefit derived from the investment. The cost-value proposition is calculated as:

Cost-value Proposition = Cost at Risk (Without Control) - Cost of Control

The outcome of the cost-value proposition provides an effective decision mechanism for the business to focus on, beyond just controlling IT risks, by counterbalancing the value toward controlling the risk.

Example Scenario Walk-through

In continuance to the risk analysis stage, multiple solutions are proposed toward treatment of risk for the review system (System X). Based on high-level analysis and judgments, the entity (along with the specialist groups) short listed two solutions. The cost of implementing Solution A for

the financial institution is US \$150,000 and Solution B is US \$100,000. Based on the solution analysis assessment questionnaire, the percentage control achieved is calculated as 82 percent for Solution A and 90 percent for Solution B.

The residual risk is calculated as $(1 - 0.82) \times 0.75 = 0.135$, i.e., 13.5% for Solution A; and $(1 - 0.90) \times 0.75 = 0.075$, i.e., 7.5% for Solution B.

The cost at risk (with control) is calculated for the proposed solution as $(0.135 \times \$42,333) = \text{US } \$5,715$ for Solution A, and $(0.075 \times \text{US } \$42,333) = \text{US } \$3,175$ for Solution B.

Based on judgments, the specialist group found the solution life for ABC's business environment to be at least four years. Hence, the solution cost corrected to annual scale for Solution A and Solution B would be $(\text{US } \$150,000 / 4) = \text{US } \$37,500$ and $(\text{US } \$100,000 / 4) = \text{US } \$25,000$, respectively. The cost of control is calculated as $(\text{US } \$37,500 + \text{US } \$5,715) = \$43,215$ for Solution A, and $(\text{US } \$25,000 + \text{US } \$3,175) = \text{US } \$28,175$ for Solution B. The cost value proposition for Solution A is calculated as $(\text{US } \$31,750 - \text{US } \$43,215) = -\text{US } \$11,465$ and for Solution B is $(\text{US } \$31,750 - \text{US } \$28,175) = \text{US } \$3,575$. As per the values derived out of the cost-value proposition exercise, Solution B reveals a positive cost-value and Solution A reveals a negative cost-value. A positive cost-value outcome provides an encouraging rationale toward selection of the solution.

Conclusion

In the current frequently changing demands of the regulatory landscape, businesses need to stay abreast of managing their IT risks. It is imperative that they modernize their traditional risk management concepts toward value-driven techniques.

The data elements derived out of this approach facilitate the business in understanding its current risk exposures and planning solutions for controlling them through a well-proven cost-value analysis technique. The value-driven approach will eventually improve an organization's capability for effectively managing its IT risks and, in turn, complying with fiduciary demands.

References

Information Security Forum, *The Standard of Good Practice for Information Security*, 2007

US National Institute of Standards and Technology, Computer Security Research Center, *Security Metrics Guide for Information Technology Systems Special*, Special Publication (SP) 800-55, 2002

ComputerWorld, ROI Knowledge Center, www.computerworld.com/managementtopics/roi

Champlain, Jack J.; *Auditing Information Systems*, John Wiley & Sons Inc., 2003

Sudhakar Sathiyamurthy, ITIL, MCSE

is a senior consultant in the IT Governance and Process Consulting (IGPC) group of i-flex Consulting, focusing on IT governance, risk and compliance. He has extensive experience in the areas of risk assessment, IT audit, process transformation, regulatory compliance and program management. He can be reached at sudhakar.sathiyamurthy@iflexsolutions.com.

New Identity Theft Regulations

By Silka Gonzalez, CISA, CISM, CISSP, CITP, CPA

The Problem of Identity Theft

Identity theft is a type of fraud that is committed when an individual uses someone else's personal information, such as Social Security numbers, account numbers and driver's license numbers, without their permission. Identity thieves can affect consumers in different ways. For example, identity thieves can obtain access to someone's bank account and transfer funds to other accounts and even incur fraudulent charges on credit card accounts. Furthermore, identity thieves can open new accounts in the customer's name, incur expenses and never pay the bills. Such fraudulent actions can have devastating effects on the credit rating of the affected consumer.

Federal Law

In 2003, the US Congress reacted to the increasing problem of identity theft by amending the Fair Credit Reporting Act with sections 114 and 315 of the Fair and Accurate Credit Transactions Act (FACT Act).

Section 114 directed various US federal agencies to issue joint regulations and guidelines regarding the detection, prevention and mitigation of identity theft. This included special regulations requiring debit and credit card issuers to validate notifications of changes of address that are followed closely by a request for an additional or replacement card.

Section 315 requires various US federal agencies to issue joint regulations and guidelines regarding policies and procedures that entities using credit reports need to use when the organization receives a notice of address discrepancy.

In November 2007, several US federal agencies issued their joint final rules and guidelines concerning identity theft red flags and address discrepancies. The agencies include the Office of the Comptroller of the Currency (OCC), Board of Governors of the Federal Reserve System (FR Board), Federal Deposit Insurance Corporation (FDIC), Office of Thrift Supervision (OTS), National Credit Union Administration (NCUA) and the Federal Trade Commission (FTC). The joint final rules and guidelines became effective on 1 January 2008. The mandatory compliance date for these final rules was 1 November 2008.

The new rules and guidelines require the following primary components:

- Development, implementation and enforcement of an identity theft prevention program
- Performance of ongoing and comprehensive risk assessments
- Development of specific policies, procedures and practices to combat identity theft issues
- Training for entity personnel
- Oversight of service providers
- Management and oversight of the program

The above components need to be properly addressed in a written and formal identity theft prevention program. The following sections expand on the basic requirements of the new rules and guidelines.

Entities That Must Have an Identity Theft Prevention Program

Financial institutions and creditors such as banks, finance companies, automobile dealers, mortgage brokers, utility companies and telecommunications companies offer or maintain one or more covered accounts. They must develop and implement a written identity theft prevention program that is designed to detect, prevent and mitigate identity theft in connection with the opening of a covered account or any existing covered account.

Covered accounts are accounts used primarily for personal, family or household purposes. They involve or are designed to permit multiple payments or transactions such as a credit card account, mortgage loan, automobile loan, margin account, cell phone account, utility account, checking account and savings account.

A covered account is also defined as any other account that the financial institutions or creditors offer or maintain for which there is a reasonably foreseeable risk to customers or to the safety and soundness of the financial institutions or creditors from identity theft, including financial, operational, compliance, reputation or litigation risks.

The program must be appropriate to the size and complexity of the financial institution or creditor and the nature and scope of its activities.

Financial institutions or creditors must perform periodic risk assessments to determine whether they offer or maintain covered accounts.

Reasonable Policies, Procedures and Practices

The program must include reasonable policies, procedures and practices to:

- Identify identity theft red flags (patterns, practices and activities that indicate possible identity theft). When identifying red flags, the entity must consider the types of covered accounts it offers and/or maintains, the methods it provides to open its covered accounts, the methods it provides to access its covered accounts, and its previous experiences with identity theft problems.
- Detect identity theft red flags. Such policies, procedures and practices must cover measures like obtaining and verifying identifying information about the individuals, authenticating

customers, monitoring transactions, and verifying the validity of change of address requests.

- Respond to identity theft red flags in a way that is commensurate with the degree of risk posed. For instance, the practices used to respond to a computer security breach compromising the data of many clients or the compromise of customer data via a fraudulent web site will have to be very different from those required to control the compromise of customer data contained on hard copy documents. The prevention and mitigation measures to respond to identity theft red flags should include the use of better logical and physical security measures, ongoing monitoring of account activity, closing selective accounts, and notifying law enforcement.
- Form a reasonable belief that a consumer report relates to the consumer about whom a report has been requested, when the entity receives a notice of address discrepancy
- Provide an address for the consumer that the entity has reasonably confirmed is accurate to the consumer reporting agency from which it received the notice of address discrepancy
- Assess the validity of a change of address if a credit card issuer receives notification of a change of address for a consumer's debit or credit card account and within a short period of time after the card issuer receives a request for an additional or replacement card for the same account

Management Must Approve, Oversee and Update the Program

The board of directors, an appropriate committee of the board of directors or a designated employee at the level of senior management must formally approve the program and must be responsible for the oversight, development, implementation and administration of the program. The board of directors or designated senior management personnel must assign specific responsibility for the program's implementation, review status reports prepared by entity personnel designated to implement the program and approve necessary changes to the program.

The program must address appropriate and effective oversight of service provider arrangements. Financial institutions or creditors should take steps to ensure that the activities of service providers are conducted in accordance with reasonable policies and procedures designed to detect, prevent and mitigate the risk of identity theft. Financial institutions or creditors should require service providers by contract to have policies and procedures to detect relevant red flags as well as report the red flags to the financial institutions or creditors.

The program must address the necessary staff training to effectively implement the program.

The program must be updated periodically to reflect changes in risks, such as changes in identity theft methods used, entity experience with identity theft problems, and changes in the business structure including a merger or hiring a new service provider.

Enforcement

The new US federal identity theft regulations are part of the recent trend for legislation and regulations to strengthen

protections for private information and prevent harm to the public. It is expected that regulators will enforce this regulation just as vigorously as they have enforced regulations issued under other statutes concerned with privacy such as the US Gramm Leach Bliley Act (GLBA).

Enforcement of these identity theft regulations will be handled by the US agencies that issued the regulations: OCC, FR Board, FDIC, OTS, NCUA and FTC. In recent years, these same US federal agencies have taken numerous enforcement actions against institutions for failure to have adequate programs to safeguard customer information. Federal regulators have taken both formal and informal enforcement actions.

The FR Board, FDIC, OCC and OTS combined have taken more than 57 formal enforcement actions in the past six years. The FTC has brought more than 14 enforcement cases in the past six years against firms for failing to maintain reasonable procedures to protect sensitive consumer data.

The following are examples of regulators' recent formal and informal enforcement actions for organizations not properly safeguarding sensitive customer information:

- **Cease and desist order**—A California-based financial institution improperly disposed of hundreds of customer loan files. A cease and desist order was issued against the institution and its service provider. Both the institution and its service provider were assessed hundreds of thousands of US dollars in civil penalties. The institution was required to notify customers of the security breach.
- **Order directing compliance with information security standards**—Examination of a state chartered bank disclosed significant computer system deficiencies and inadequate controls to prevent unauthorized access to customer information. The bank was required to perform a formal risk assessment of internal and external threats and to ensure that computer user access levels were appropriately restricted.
- **Enforcement actions related to employees**—A retail credit card bank's information was compromised. The FTC and the bank regulatory agency reviewed identity theft complaints and determined that the information was misused. The bank was ordered to notify its customers. The financial regulator imposed on an employee a lifetime prohibition from the banking industry plus civil penalties.
- **Enforcement actions related to employees**—A federal regulator found that a large financial institution had hired a convicted felon who engaged in crimes related to identity theft. The regulatory agency directed the financial institution to improve its employee screening policies, procedures, systems and controls.

Audits and enforcement of the new identity theft regulations began as of 1 November 2008, the date by which compliance is mandatory. Organizations and individuals should expect similar types of sanctions and fines as those that various regulatory agencies are already imposing to enforce security-related US federal regulations, such as GLBA.

Conclusion

The new identity theft regulations reflect the strong concern in preventing and fighting the crime of identity theft. The regulations are different from other security-

related federal regulations in that these regulations focus only on identity theft, which is only one of the many security problems that an organization can face. These regulations also differ from other security-related regulations because they cover a broader range of industries, rather than focusing on specific industries. Still, the identity theft regulations need to be applied in conjunction with other existing federal regulations, such as GLBA, because these regulations also aim to protect individuals' private information and have related requirements.

The new identity theft regulations are a positive step toward protecting individuals' private information and fighting fraud. These regulations demand the use of controls to not only prevent identity theft, but also to detect

and respond to identity theft incidents as they are taking place. They emphasize that organizations must respond appropriately to identity theft red flags. Still, criminals will continue to adjust their methods for stealing others' identities and money. Therefore, to effectively prevent identity theft, organizations will need to be vigilant beyond the specific requirements of the new regulations.

Silka Gonzalez, CISA, CISM, CISSP, CITP, CPA

is the president of Enterprise Risk Management, one of the leading providers of IT security, risk management, IT audit, computer forensics, regulatory compliance and SAS 70 services to global businesses, with offices in the US and India. She can be reached at info@emrisk.com.



**EXCEPTIONAL TRAINING
AT YOUR OWN PACE**
— **AT YOUR OWN PLACE**

The ISACA® e-Learning Campus and COBIT Campus

Discover online training from a trusted source, delivering self-paced online learning courses to information systems (IS) and IT professionals anywhere, any time. Gain knowledge while earning valuable CPE credits.

e-Learning Campus—NEW

Featuring the CISA® Online Review Course—a choice of six modules leveraging the latest materials and guidance from Certified Information Systems Auditor™ (CISA®) professionals and subject matter experts. Prepare for the CISA exam or accumulate CPE credits.

COBIT Campus

Ensure IT is working effectively to minimize risks and maximize technology investments. Master *Control Objectives for Information and related Technology* (COBIT®) and utilize this knowledge for effective implementation at your enterprise.

Discounted pricing available exclusively to ISACA members.

Visit www.isaca.org/elearning and register for a course today!



Issues With Auditing the Systems Development Process

By Dave Henderson, Ph.D.

Toward the end of 1995, before replacing an aging mainframe system with an enterprise resource planning (ERP) software package, FoxMeyer had US \$5 billion in revenue per year and was a leader in the pharmaceutical industry. By early 1996, the ERP system was not handling customer orders as anticipated and, as a result, millions of dollars of customer orders were mismanaged. FoxMeyer announced it would take a US \$34 million charge for uncollectible costs related to customer orders and subsequently went into Chapter 11 bankruptcy proceedings.¹

In a similar instance, senior managers at Oxford Health failed to ensure that the company's new billing system could handle current billing requirements even though its billing system was a critical component in the company's future growth and profitability. Eventually, the billing system failed, resulting in heavy losses and causing Oxford Health's stock price to decrease from US \$68 to US \$26 in one day.²

These are not isolated examples, and they accurately illustrate the catastrophic impacts a failed software project can have on an organization, including damaging shareholder value and even forcing bankruptcy.³ The appropriate use of a formal systems development methodology⁴ is essential for mitigating the software project failure risks associated with systems development projects.⁵ Although methodologies are vital controls during systems development and warrant the attention of information systems (IS) auditors, some development teams use them inappropriately.

The purpose of this article is to discuss how inappropriate methodology use can hinder risk mitigation strategies during the systems development process. The article will conclude with how IS auditors can respond.

The Importance of a Methodology

A systems development methodology, a specific instance of the systems development life cycle (SDLC), is defined as "a systematic approach to conducting at least one complete phase of information systems development, consisting of a recommended collection of phases, techniques, procedures, tools and documentation aids."⁶ Examples of methodologies include the Rational Unified Process, Extreme Programming, the Waterfall methodology as well as numerous in-house methodologies that are proprietary to a particular organization.

Mitigating risk during systems development is an important consideration for IS auditors when reviewing the

systems development process. Systems development carries numerous potential risks including:

1. Inadequate controls in the development process
2. Schedule and budget overruns
3. User requirements not being met by the application system
4. Inadequate stakeholder involvement⁷

Because a methodology can help mitigate risk during systems development, IS auditors should ensure that development teams use it appropriately. Without the appropriate use of a methodology, the systems development process may be controlled loosely, thereby making it difficult to mitigate these risks. For example, if a development team builds an application system using an inappropriate methodology, the application may fail to meet user needs—a significant risk during systems development.⁸

Methodologies also warrant the attention of IS auditors, because the existence of a documented methodology suggests a more dependable IT operating environment and provides

*The existence of a
documented methodology
suggests a more dependable
IT operating environment.*

appropriate documentation for each phase of the systems development process.⁹ Furthermore, IS auditors may need to consider the existence of a methodology to ensure compliance with the Capability Maturity Model Integration (CMMI) standards¹⁰ or International Organization for Standardization (ISO) standards.¹¹ Finally, methodologies are an important consideration for IS auditors,

because more mature systems development practices (e.g., use of a methodology), as required for CMMI compliance, can facilitate Sarbanes-Oxley compliance.¹²

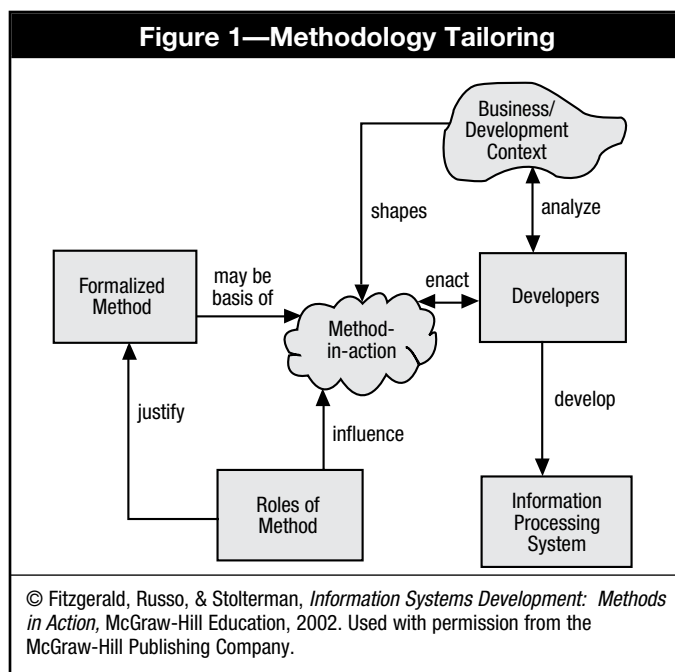
Role of IS Auditing in the Systems Development Process

IS auditors typically execute three types of reviews of the systems development process: a preimplementation review, a parallel review and a postimplementation review.¹³ During a preimplementation review, the IS auditor investigates the proposed methodology and considers its applicability and the potential risks associated with the systems development project. In a parallel review, the IS auditor reviews the pertinent stages of the methodology as they proceed and, subsequently, calls attention to possible risks and provides suitable risk mitigation approaches. Finally, during a postimplementation review, the IS auditor reviews the relevant stages of the methodology after the systems development project has been completed. Furthermore, the IS auditor emphasizes issues faced during the systems development project and provides recommendations for

improvement. When conducting preimplementation, parallel or postimplementation reviews of the systems development process, IS auditors should confirm that development teams have adopted a valid methodology and that they are using it appropriately.¹⁴

Methodology Tailoring

Methodology tailoring, the purposeful customization of the organization's formal methodology for the characteristics of a particular development context, affects how development teams use a methodology and represents an important issue for IS auditors to consider.¹⁵ Rather than following a methodology rigorously, developers typically modify a given methodology based upon several factors, including the organization's adopted methodology, the development context, the roles of the methodology, the type of system being developed and developer-related factors (see **figure 1**).¹⁶ These factors interrelate to create a tailored methodology for every systems development effort.¹⁷



The “formalized methodology” factor of the Fitzgerald framework illustrated in **figure 1** refers to the formal methodology adopted by the organization. The formal methodology serves as a foundation for the tailored methodology. The “roles of method” factor in **figure 1** refers to how a methodology can play a rational role or a political role. Examples of rational roles include breaking down the systems development process into logical steps, assisting project management and increasing discipline in the systems development process. Examples of political roles include increasing the professionalism of systems development, providing a paper trail of the development process, meeting a certification established by an external organization (e.g., CMMI, ISO) and fulfilling a client requirement.¹⁸

The “business/development context” factor shown in **figure 1** is defined as the environment within which the systems development process occurs. Characteristics of the development context can influence how development teams use the methodology. For example, the development of a

large system may require different collaboration tools and techniques than the development of a small system.¹⁹

The type of application system being developed can also affect how developers use the methodology. The development of a unique and highly complex system, for example, may require a more disciplined process than the development of a simple application system.²⁰

Finally, developer-related factors can influence how a development team uses a methodology.²¹ Due to individual differences, developers may use the same methodology differently for a given situation. Developer experience is an important developer-related factor that can influence how a methodology is used. Experienced developers perceive methodologies as frameworks, rather than recipes for systems development to be followed strictly.²² Accordingly, experienced developers can draw upon their knowledge to appropriately customize a given methodology to the development context.²³ Inexperienced developers, on the other hand, may find a methodology to be a useful handbook for learning the organization's system development processes and are more likely to follow a methodology rigorously to make up for their lack of self-confidence.²⁴

Methodology tailoring has several implications for IS auditors when reviewing the systems development process. First, IS auditors should recognize that purposeful methodology tailoring can be desirable because by skipping steps or techniques recommended by the methodology, that may not be applicable to the development context, the development team may execute a more efficient development process.

Second, IS auditors should recognize that the potential exists for some inexperienced development teams to blindly follow a methodology without tailoring it to the development context. Due to their lack of self-confidence, inexperienced developers are more prone to goal displacement—when a developer strictly adheres to the methodology to the detriment of actual development.²⁵ When inexperienced developers follow a methodology too closely, they may perform unnecessary steps during systems development. For instance, completing a lengthy feasibility study, as may be recommended by an organization's formal methodology, may be unnecessary for a small application system. Performing unnecessary steps during the systems development process, in turn, raises the possibility that the systems development project may not be delivered on time—a potential risk IS auditors should consider during the systems development process.

IS auditors can employ several strategies for reducing the risks associated with inappropriate methodology use. First, they should take an active role in the systems development process.²⁶ By observing how the development team is using the methodology, IS auditors can ensure that the development team is purposefully tailoring the methodology for the development context, rather than rigorously following every step recommended by the methodology. Second, IS auditors should also ensure that experienced development team members, rather than inexperienced team members, customized the methodology. Third, IS auditors should ensure that the development team documented adaptations to the methodology and provided adequate rationale for each adaptation.²⁷

Methodologies and Organizational Politics

Although development teams can use a methodology to mitigate risk during systems development and achieve higher software quality, they can also use it to achieve political objectives.²⁸ Specifically, development teams may use a methodology to show others that systematic development processes are being used²⁹ or to block user requirements.³⁰

When auditing the systems development process, IS auditors should review documentation to ensure that a formal methodology exists and that deliverables have been created with the use of that methodology. Reviewing documentation, however, may not be enough. Development teams may use a methodology to give the impression that company standards and guidelines have been followed.³¹ When development teams use a methodology in this manner, however, they may use it in a superficial way and add or change documentation to give the appearance that they followed the methodology.³² Consequently, the mere existence of documentation for a methodology does not imply that the development team has used the methodology in an appropriate manner. IS auditors, therefore, need to go beyond documentation and employ additional data-gathering techniques, such as interviewing members of the organization outside the development team. For example, if a development team is using the traditional Waterfall methodology, IS auditors could interview users to see if they formally signed-off on requirements before the coding phase began. Furthermore, IS auditors should take an active role in the systems development process. By participating in the systems development process, IS auditors can ensure that development teams create the appropriate systems documentation when it should be created.

In addition to changing documentation to give the appearance that a methodology was used, development teams may use a methodology to block changes to requirements.³³ For example, the traditional Waterfall methodology discourages changes to requirements after the requirements analysis phase has been completed. Thus, development teams could use the authority embedded in the methodology to prevent requirements changes if they are proposed in phases of the methodology after the requirements analysis phase (e.g., the coding phase). Using a methodology to block changes to requirements may result in an application system that does not meet user needs—a significant risk during the systems development process. To mitigate this risk, IS auditors should interview members of the organization outside the development team, actively contribute to the systems development process and ensure that the rationale for choosing a certain methodology is thoroughly documented.

Conclusion

While this article discusses potential audit risks associated with inappropriate methodology use, its purpose is not to indict all development teams. Certainly, many development teams recognize the importance of methodologies and use them in an informed and logical way.³⁴ However, given the potential for development teams to use a methodology inappropriately, it is important for IS auditors to understand how to mitigate risks associated with inappropriate

methodology use. By actively participating in the systems development process and interviewing stakeholders outside the development team, IS auditors can help ensure that the full potential of the methodology to mitigate many of the risks associated with systems development is realized.

Endnotes

- ¹ Jesitus, John; “Broken Promises? FoxMeyer’s Project Was a Disaster. Was the Company Too Aggressive or Was It Misled?,” *Industry Week*, vol. 246, no. 20, 1997, p. 31
- ² Charette, Robert; “Why Software Fails, Continued,” *IEEE Spectrum Online*, September 2005, <http://spectrum.ieee.org/sep05/1685/2>
- ³ Hettigei, Nandasena T; “The Auditor’s Role in IT Development Projects,” *Information Systems Control Journal*, vol. 4, 2005
- ⁴ For simplicity, a systems development methodology is referred to in this article as a methodology.
- ⁵ Singleton, Tommie; “Systems Development Life Cycle and IT Audits,” *Information Systems Control Journal*, vol. 3, 2004
- ⁶ Siau, K; Xin Tan; “Evaluation Criteria for Information Systems Development Methodologies,” *Communications of the AIS*, vol. 16, 2005, p. 863
- ⁷ ISACA, IS Auditing Guideline G23, System Development Life Cycle (SDLC) Reviews, 2003, www.isaca.org/standards, p. 2
- ⁸ Hall, James; Tommie Singleton; *IT Audit and Assurance, 2nd Edition*, Thomson-Southwestern Publishing, 2005
- ⁹ *Op cit*, Singleton, 2004
- ¹⁰ Duggan, Evan; “Silver Pellets for Improving Software Quality,” *Information Resources Management Journal*, vol. 17, no. 2, 2004, p.1
- ¹¹ Fitzgerald, Brian; “An Empirical Investigation Into the Adoption of Systems Development Methodologies,” *Information & Management*, vol. 34, no. 6, 1998, p. 317
- ¹² Janssens, Laurent; Peter Leeson; “Auditing CMMI Maturity and Sarbanes-Oxley Compliance,” *Information Systems Control Journal*, vol. 3, 2007
- ¹³ *Op cit*, ISACA, G23, p. 4
- ¹⁴ IT Governance Institute, *IT Control Objectives for Sarbanes-Oxley, 2nd Edition*, 2004, www.isaca.org/sox
- ¹⁵ Fitzgerald, Brian; Nancy L. Russo; Erik Stolterman; *Information Systems Development: Methods in Action*, McGraw-Hill, 2002
- ¹⁶ *Ibid.*
- ¹⁷ *Ibid.*
- ¹⁸ *Ibid.*
- ¹⁹ *Ibid.*
- ²⁰ *Ibid.*
- ²¹ *Ibid.*
- ²² Fitzgerald, Brian; “The Use of Systems Development Methodologies In Practice: A Field Study,” *Information Systems Journal*, vol. 7, no. 3, 1997, p. 201
- ²³ *Ibid.*
- ²⁴ *Ibid.*
- ²⁵ *Op cit*, Fitzgerald, Russo and Stolterman, 2002
- ²⁶ *Op cit*, Hettigei

- ²⁷ *Op cit*, ISACA, G23
- ²⁸ Robey, D; M. Lynn Markus; "Rituals in Information System Design," *MIS Quarterly*, vol. 8, no. 1, 1984, p. 5
- ²⁹ Nandhakumar, J.; David E. Avison; "The Fiction of Methodological Development: A Field Study of Information Systems Development," *Information Technology & People*, vol. 12, no. 2, 1999, p. 176
- ³⁰ Wastell, D.; "The Fetish of Technique: Methodology as a Social Defense," *Information Systems Journal*, vol. 6, no. 1, 1996, p. 25
- ³¹ *Op cit*, Nandhakumar
- ³² *Op cit*, Fitzgerald, Russo and Stolterman, 2002
- ³³ *Op cit*, Wastell
- ³⁴ *Op cit*, Fitzgerald, 1997

Author's Note:

The author would like to acknowledge the ISACA SC Midlands (Columbia, South Carolina, USA) Chapter for its helpful comments on a presentation based on this paper. The author would also like to acknowledge Brad Trinkle of the College of Charleston and Melissa Walters of the University of Tampa (Florida, USA) for their suggestions on earlier versions of this paper.

Dave Henderson, Ph.D.

is an assistant professor of accounting at the College of Charleston (South Carolina, USA), where he teaches managerial accounting, accounting information systems, IT governance and systems and infrastructure life cycle management, and information systems security and control. He has accumulated more than 10 years of experience in the IT field in various roles including financial analyst, financial systems developer and project manager. He has presented several articles on systems development at various accounting and information systems conferences.

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.

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

Monitoring Privileged Application Users in Oracle Applications Environment

By Jeffrey T. Hare, CISA, CIA, CPA

Enterprise resource planning (ERP) systems have changed the dynamics of companies' enterprise applications in many ways. One of the critical benefits of ERP systems is the flexibility they provide so that they can be implemented in a variety of companies and organizations from a small municipal government to a multinational, multilingual manufacturing firm. If implementing the system in a vanilla environment, the same set of code can be used by hundreds of different types of companies. The brilliance of ERP systems is that they have code that can be manipulated by someone without any programming knowledge through a user interface (i.e., form or web page). The behavior of the code is changed by the various system configuration (i.e., setups) settings. Perhaps this flexibility is also one of the greatest curses of an ERP system as well, because, if poorly configured, it can be a disaster for a company.

One of the most important elements in a successful ERP implementation is having the right resources to configure and maintain the system. During an implementation, the right team needs to be in place to help design and transition to the ERP system. That team should know the system very well, including its limitations, and be able to tailor the system to fit the business requirements and recommend extensions or customizations only when necessary.

Enter the real world. . . . For many enterprises, by the time the system is live, it is either over budget or the enterprise has reduced its scope, or both. The migration to an ERP system is usually far more difficult and time-consuming than most enterprises recognize. Often, the postimplementation support budget has been eaten up and many of the staff members allocated to the project are supposed to go back to their real jobs.

In spite of the emphasis on internal controls in this post-Sarbanes-Oxley world, another reality is that many projects put little emphasis on the design of the applications and security to meet compliance requirements.

The combination of these challenges leaves companies with a need to support the applications in a post-go-live environment, faced with significant support issues. Aimed at trying to address these challenges, companies grant privileged users nearly unlimited access to the applications, with little control or accountability over their use of the applications.

The aim of this article is to provide awareness of risks related to these privileged users as well as guidance on how to address some of the risks.

Scoping the Problem

The reality of many companies' postimplementation environment is those that support the system (typically

business analysts and developers, together referred to as privileged users) often are given broad access to the applications and the database layers. Many privileged users have access to powerful superuser or manager roles (note that the term role will be used interchangeably in spite of the fact that many companies have not designed their security based on a role) or have custom-built roles that are attached to the same menus as the seeded superuser or manager roles. For example, privileged users supporting the Payables module in Oracle's eBusiness Suite could be granted access to the Payables Manager role or they could have a custom role. The Payables Manager role is associated with the AP_NAVIGATE_GUI12 menu. Often, in lieu of granting access to the Payables Manager role, a custom role is built called ABC Payables Manager (where ABC is the company name) and that role is associated with AP_NAVIGATE_GUI12 menu. In some cases, certain elements of the AP_NAVIGATE_GUI12 menu are excluded through the use of menu or function exclusions to remove certain functionality from being accessed by the privileged user. In some cases, however, there are no exclusions, which leaves the privileged user with the same access as if they had been granted the Payables Manager role.

The net result is the privileged user is left with significant access to maintain master data, create transactions and make changes to critical foundational setups. In the example above where the privileged user is granted access to the ABC Payables Manager menu, the privileged user may have the ability to enter a supplier, enter an invoice and generate a payment against the invoice. This would be a serious fraud risk noted by an auditor or anyone with a background in internal controls design.

Additionally, the access the privileged user has to critical foundational setups may leave the user with the ability to change the business process, compromise the defined controls and/or circumvent the company's change management process. For example, he/she could alter the Allow Address Change setting in the Payables Options form to give him/her the ability to change the supplier address on a check when issuing a manual payment.

To monitor these privileged users, management would benefit from an audit trail of all activity for these privileged users, but the design of ERP systems such as Oracle's eBusiness Suite and SAP does not allow for such an audit trail. Throughout most of the application, the database stores only the most current values, the created-by and last-updated-by information. This challenge can be illustrated, for example, through the Journal Sources form, which is

a critical foundational setup that controls the ability to manipulate journal entries from subledgers and whether or not those journals are subject to workflow approvals in Oracle's e-Business Suite.

Figure 1 is a screen shot of the Journal Sources form.

Figure 2 is an example of how some of this data would look in the GL_JE_SOURCES table (these are not actual column names, but an illustration of the issue).

The challenge when monitoring privileged users is to provide an audit trail of all activity they performed while logged into the production environment. For illustration purposes, Mary Smith is the privileged user and is supporting the GL module. A journal entry is imported from the Receivables module and the controller asks to change the journal entry before it is posted. So, a call is placed to Mary

Smith to uncheck the Freeze Journals button so the journal entry can be updated in the GL. The values after this change are shown in **figure 3**.

Then, after the change is made to the journal, the Freeze Journals button is set back to Yes. The values would then appear at the database level as shown in **figure 4**.

When the database is queried to determine what has changed, it will show that the Last Updated By and Last Updated Date values were changed by Mary Smith. However, the data in the Freeze Journal column is exactly the same as it was prior to Mary's changes. Based on the data stored in the database, there is no way of identifying the changes made by Mary.

What about an audit trail? Is there not a mechanism to store the changes that Mary made when she updated the

Figure 1—Journal Sources Form

Source	Description	Require Journal Approval	Freeze Journals	Import Journal References	Effective Date Rule
Receivables	Accounts Receivable System	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Roll Date
Recurring	Recurring Journal Entry	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Roll Date
Revaluation	Revaluation Journal Entry	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Roll Date
Revenue	Revenue Accounting System	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Roll Date
SM_Journal Source	SM_Journal Source	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Roll Date
SN SOURCE	SN SOURCE	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Leave Alone
SS SOURCE		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Roll Date
SSA PAYABLES	SAGAR PAYABLES IMPORT	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Roll Date

Figure 2—Data in the GL_JE_SOURCES Table

Source Name	Description	Freeze Journals	Require Journal Approval	Last Updated By	Last Updated Date
Receivables	Accounts Receivable System	No	No	DOEJ	01-Jan-06

Figure 3—Values of GL_JE_SOURCES Table After Changes

Source Name	Description	Freeze Journals	Require Journal Approval	Last Updated By	Last Updated Date
Receivables	Accounts Receivable System	Yes	No	SMITHM	01-Dec-07

Figure 4—Values at the Database Level Following Changes

Source Name	Description	Freeze Journals	Require Journal Approval	Last Updated By	Last Updated Date
Receivables	Accounts Receivable System	No	No	SMITHM	01-Dec-07

Freeze Journals checkbox and then changed it back to its original value? The answer is no. Out of the box, there is no such functionality, as is the case in many mainframe systems. There is no “audit all” functionality that can be turned on to monitor changes made by a privileged user.

So the question is: what risks related to access provided to privileged users exist and what type of monitoring can be done?

Four categories of risks will be discussed here:

1. High-risk single functions
2. Segregation of duties, where privileged users can compromise the business process (to manipulate results or commit fraud) because of their access to two or more functions
3. Sensitive data
4. Change management process

High-risk Single Functions

There are a variety of high-risk single functions to which a privileged user would have access. Some of these functions are transactional in nature, such as the Enter Suppliers and Enter Invoices functions. Some are foundational setups such as Payables Options and Bank Account.

There is no “audit all” functionality.

Segregation-of-duties Risks

This is the area that most people think of when considering risks in access controls, in general, and access by privileged users, in particular. Returning to the earlier example, in the Payables Manager responsibility, a privileged user has a broad array of access to payables forms including the ability to enter a supplier, enter an invoice against that supplier, and generate a payment against that supplier. That user also has access to a wide variety of foundational setup menus, such as payables options and financials options.

Sensitive Data

Another area that many companies fail to take into account is sensitive data. Does the access allowed by the privileged user allow access to sensitive data? To answer that question, the company must define what data are sensitive, identify where those data are stored, and identify by what means those data can be accessed.

Does management feel comfortable with privileged users having access to sensitive employee data, such as home address and bank account information, that may be stored in other areas of the application, such as Payables, to allow for the processing of expense reports? Do database logins restrict access to sensitive employee payroll and bank account data contained in the HR tables? Has access to sensitive data that can be obtained by the running of standard or custom reports been fully analyzed?

Change Management Process

The last area of risk to be discussed here is the change management process. Many companies narrowly define change management by taking into account only object or data changes. However, the intent of change management should be to protect the business process and its related controls, not just the objects (i.e., code) and the data. Therefore, the change management process should take

into account critical forms-based changes that can have a significant impact on the integrity of the business process or the controls related to that business process.

The following examples may help illustrate the risk. First, in Oracle’s e-Business Suite, the Purchasing Options form allows a user to define the matching requirements (two-, three- or four-way) that default on the PO lines (even though they can be overridden by the buyer). If the company has a requirement that all POs go through a three-way match and this setting is changed, it changes the business process (i.e., invoices matched to POs will no longer go on matching hold waiting for a receipt) and the controls (i.e., the company will likely fail testing of that control during the next management or Sarbanes-Oxley section 404 testing cycle). A second example is the value sets related to the chart of accounts (or Accounting Key flexfield). If a user in Fixed Assets is trying to maintain a Location flexfield, but makes an unauthorized change to the value set of one of the segments in the chart of accounts, this could cause a control deficiency. Both the Purchasing Options and Value Set Maintenance forms may be forms that a privileged user has in the production environment. Both changes, perhaps, should go through the change management process, so that the changes are authorized and approvals are properly documented.

The privileged user could also have access to forms that allow embedded Structured Query Language (SQL) statements that could manipulate data (INSERT, UPDATE, DELETE, etc.) or database structures (ALTER, TRUNC, DROP, etc.).¹

Using Database and OS Logins

The definition of privileged users can also extend to those who can manipulate data through database and operating system logins. While most of the remainder of this article relates to access through the applications, one needs to consider the ability to manipulate or access data through these means as well. To the extent that mechanisms are put in place to monitor access of privileged users at the application level, some mechanisms can also provide some monitoring of database and OS users. As such, the mechanisms could be accomplishing multiple objectives and should be coordinated with those that are designing monitoring controls for privileged users at those levels, as well.

Options for Monitoring Privileged Users

With these risks in mind, how are companies monitoring privileged application users? This article looks at the pros and cons of three common ways to monitor privileged users:

1. Use of sign-on Audit functionality
2. Selective auditing of high-risk setups and master data
3. Monitoring of transactions entered

Use of Sign-On Audit Functionality

Oracle eBusiness Suite has a profile option called “Sign-On:Audit Level.” This can be set at various levels including None, User, Responsibility and Form. Oracle recommends, and many experts agree, that this profile option is most

appropriately set at the Form level. This provides for the most information to be collected since Form is the lowest level of detail allowed. When set at the Form level, this tracks the responsibility and form used when a user, including privileged users, logs into the application. A Sign-On Audit Forms report can be run to identify the forms accessed by the user.

Some companies use this functionality to track the forms that the privileged users access when they log into the application. Some companies also require that privileged users log their activity via a help-desk ticket or other mechanism and compare the help-desk ticket logs to the forms they use (via the Sign-On Audit Forms report) to make sure they are consistent. Employees are questioned about any discrepancies or unusual activity.

The benefit of using this method is that the functionality is built in to the core applications (i.e., seeded functionality) and, therefore, is free. This method provides some limited accountability.

The limitation of using this functionality is that the reporting tells nothing about what was done when the user accessed the form. The Sign-On Audit Forms report merely tells that the form was opened; it does not indicate whether the user solely viewed the data or made changes to the data. Therefore, if the privileged users logged that they went into the Suppliers form to look at some settings for a particular supplier, it is unknown whether they only looked at the supplier or if they set up a fictitious supplier.

*The reporting tells nothing
about what was done.*

Selective Auditing of High-risk Setups and Master Data

The next two layers of monitoring require that a risk assessment process be performed to identify the areas of risk within the application. A proper risk assessment process will take a look at each of the modules and overall system settings to identify which access has the greatest risks to the company.²

Some functions have risk for all companies. Accessing certain forms that allow SQL statements to be embedded in them, and then executed, have risks for all companies. Access to maintain certain master data, such as Remit-To Addresses and Banks, has risk for all companies. For these types of transactions, the company will want to have a detailed audit trail of all changes so that it can properly audit the changes. Because of the lack of a detailed audit trail, one particularly high-risk situation (remember the Journal Sources example) is where the data are changed by a privileged user then changed back. For example, if a privileged user knew when a payment run was being scheduled for a large vendor that was paid via an automated clearinghouse (ACH), the user could change the bank account to a fictitious bank account number on the day prior, and then change it back after the payment batch process was run. Absent a detailed audit trail of the changes, it would be difficult to piece together the audit history of that fictitious payment.

However, risks of access to many functions can be identified only by taking into account the mitigating controls for each particular company. For example, if the company has a good process for reviewing supporting documentation and assessing the validity (i.e., checking for fraud) of the

expenditures before checks or ACH transactions are sent, then the entry of a fictitious supplier may not seem risky to the company, based on the likelihood that the review would catch fictitious expenditures. However, if the review process looks at only checks over a certain monetary amount (i.e., significant expenditures), the company may be at risk for fraud below the defined "significant amount" and want to put into place some additional procedures such as an audit of the supplier entry process.

Once the high-risk areas are identified, the company may want to put in some additional monitoring controls to make sure the privileged users do not compromise the processes and controls or allow privileged users to commit fraud while performing their role. The monitoring may take the form of the use of alerts (which are fired typically based on a trigger) or a trigger or log-based auditing solution. The use of a database trigger or various types of logs (network or redo) is typically secured from most privileged users because most privileged users do not have the ability to manipulate the audit data or logs. However, the risk exists that a developer performing support functions could have access to the Define Alerts screen and could disable the alert when going into certain high-risk forms to evade an audit trail. If using alerts, any changes to alerts should be tracked by someone other than the developer (i.e., the database administrator [DBA]) and/or be audited for any changes such as disabling.

Both triggers and auditing through log files potentially have benefit for operating system (OS) and DBA users, but may not be foolproof because of the ability to manipulate the data, triggers or logs using other logins (database or OS). Therefore, companies need to do the research and know what other capabilities the privileged users have before relying on audit trails.

Monitoring of Transactions Entered

The next possible layer of monitoring of privileged users is the monitoring of transactions. For discussion purposes, the transactions have been segregated from high-risk setups and master data because the volume of data on transactions such as POs and AP Invoices is significantly higher than the volume of data for setups and master data. Therefore, the technology for monitoring high-volume transactions needs more discussion.

Even though transactions can be monitored via triggers, they typically are not because of the possibility of performance issues. Some vendors allow leverage FGA or have custom triggers that allow for conditions to be placed on them such that the trigger body would fire only under certain conditions (e.g., when the transaction is being performed by a specific privileged user). Under the right circumstances, triggers could be used even on high-volume transaction tables.

The use of logs to monitor transactions entered by privileged users may be a sound technique depending on the types of logs and other capabilities of the privileged users. Logs have very little system performance risk, so they are ideal for transaction monitoring on high-volume tables, especially if the company has purchased a log-based solution for other purposes (e.g., monitoring activities of key DBAs).

The use of standard tables to monitor transactions entered by privileged users is a reasonable solution as well. Whereas in master data there are risks such as maintaining the data and then changing them back (as discussed earlier), there is less risk of this when entering transactions. Therefore, reports developed against the Created By and Last Update By columns should capture most of the significant activity, especially if there is strong monitoring of critical master data and setups.

Who Owns the Tools?

One final topic to be considered relates to who implements and owns the tools. Generally, the privileged users the company is trying to monitor either are developers or business analysts. In a larger environment, either finance or corporate governance would own the configuration and maintenance of the tool. The other option is to have the DBA staff own it, since they are likely not privileged users at the application level. DBAs typically are the ultimate privileged users because of their ownership of the Apps login at the database level.

Part of the decision process is what tool or tools would be used to monitor the privileged users. Some tools have a user interface that is intuitive for a functional user in finance or corporate governance, and some tools would best be maintained by someone with a technical background, such as a DBA. In any case, the company does not want the fox watching the chicken coop, so the analysts or developers should not be involved in the implementation or maintenance of the application. Also, internal audit needs to maintain its independent role and, therefore, should not be involved.

Ideally, the group in charge of the risk assessment process is also responsible for implementing the controls to monitor the risks identified. Usually, this is either finance and accounting personnel or a separately defined corporate governance group.

Conclusion

In an ideal world, a company would not need to grant excessive access to privileged users in a production environment. Many companies, though, have chosen to grant broad access to a limited number of users to support and maintain the system. The hope is that they have assessed the risk appropriately and put in proper monitoring mechanisms to reduce the various risks excessive access causes.

Endnotes

¹ See detailed list of such forms in Oracle's Metalink document 189367.1, and some assessment in Oracle's Metalink note by joining the Internal Controls Repository at <http://tech.groups.yahoo.com/group/oracleappsinternalcontrols/>.

² To understand the full scope of what it takes to perform a proper risk assessment, see the white paper titled "Risk-based Assessment of User Access Controls and Segregation of Duties for Companies Running Oracle Applications" from the Oracle Users Best Practices Board at www.oubpb.com.

Jeffrey T. Hare, CISA, CIA, CPA

is the founder of ERP Seminars (www.erpseminars.com) and the Oracle User Best Practices Board (www.oubpb.com) and has written various white papers on internal controls and security best practices in an Oracle Applications environment. He has presented white papers to various user groups throughout the country. He is the author and presenter of the seminar, Internal Controls and Security Best Practices in an Oracle Applications Environment. His background includes Big 4 experience, more than six years of experience in chief financial officer/controller roles, and having been in the Oracle Applications space since 1997. Hare can be reached at jhare@erpseminars.com.



Protect Your Company's Important Information and Systems

Let Georgia Tech provide the training you need to ensure your company is protected.

Is your company protected from potential disasters, man-made or natural?
Do you have an action plan in place if something were to happen?

Georgia Tech's Managing Information Security training helps you:

- Gain a better understanding of how information security has evolved
- Learn to apply these changes and updates to your company
- Prepare for the CISSP exam

Georgia Tech's information security program is comprised of seven courses offered throughout the year. Upon completion of all seven courses, a Georgia Tech certificate is earned.

SAVE 15%

Learn how at
www.dlpe.gatech.edu/it/isad



Prepare for the 2009 CISM Exams

ORDER NOW—2009 CISM® Review Materials for Exam Preparation and Professional Development

To pass the Certified Information Security Manager® (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 for more details).

CISM Review Manual 2009

ISACA

The *CISM® Review Manual 2009* is a comprehensive reference guide designed to assist individuals in preparing for the CISM exam and individuals who wish to understand the roles and responsibilities of an information security manager. The manual has evolved over the past five editions and now represents the most current, comprehensive, globally peer-reviewed information security management resource available.

In response to the evolving field of information security management, the extensively expanded and revised 2009 version of the *CISM Review Manual* continues to move away from the topic of technology and closer to the strategic governance and management aspects of security. There is increasing emphasis on the overarching concepts essential for effective information security management in addition to focusing on the critical thinking and sound judgment required for the development and management of increasingly massive and complex security systems and related processes. This publication includes a new and expanded approach to the development of effective security management metrics, based on research projects sponsored by the IT Governance Institute® (ITGI™). There is a substantial increase in the scope and depth of coverage on the subject of risk management. An expanded focus and structural improvement is included for information security program development as well as a greater concentration on architecture and metrics. The improved approach to management metrics has been carried through to the section on information security management providing processes to improve overall effectiveness. Also included are case studies to assist a candidate in understanding current practices, definitions of terms most commonly found on the exam, practice questions similar in content to the certification exam and references to additional study materials. This manual can be used as a stand-alone document for individual study or as a guide or reference for study groups and chapters conducting local review courses. It is a primary reference resource for information security managers seeking global guidance on effective approaches to governance, risk management, program development, management and incident response.

The 2009 edition has been developed and is organized to help prepare the CISM candidate in understanding the essential concepts and studying the following job practice areas:

- Information security governance
- Information risk management
- Information security program development
- Information security program management
- Incident management and response

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

CISM Review Questions, Answers & Explanations Manual 2009

ISACA

The *CISM® Review Questions, Answers & Explanations Manual 2009* consists of 450 multiple-choice study questions that have previously appeared in the *CISM® Review Questions, Answers & Explanations Manual 2008* and the *2008 Supplement*. These questions are not actual exam items, but are intended to provide 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 2009*.

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

- Sorted by job practice area
- Sample 200-question exam

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

CISM Review Questions, Answers & Explanations Manual 2009 Supplement

ISACA

Developed each year, the *CISM® Review Questions, Answers & Explanations Manual 2009 Supplement* is recommended for use when preparing for the 2009 CISM exam. Each edition consists of 100 new sample questions, answers and explanations based on the current CISM job practice areas, using a process for item development similar to the process 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-9ES English Edition
CQA-9JS Japanese Edition
CQA-9SS Spanish Edition

CISM Practice Question Database v9

ISACA

The *CISM® Practice Question Database v9* combines the *CISM Review Questions, Answers & Explanations Manual 2009* with the *CISM Review Questions, Answers & Explanations Manual 2009 Supplement* into one comprehensive 550-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 2009*. 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 80 MB of available space
- CD-ROM drive
- Display with recommended resolution of 1024 x 768

MDB-9 English Edition—CD-ROM
MDB-9W English Edition—Web site download

To order CISM review material for the June/December 2009 exams, see the order form on page S-8 in this Journal or visit the ISACA web site at www.isaca.org/cismbooks.

Black Box Testing:

Its Fundamental Concepts and Problems

By Pak-Lok Poon, Ph.D., CISA, CSQA, MACM, MIEEE

In today's information age, organizations rely heavily on and are being affected by every kind of information system flooding into the business world. On the other hand, enough horror reports of faulty systems and their associated problems and catastrophes, resulting in inconvenience, annoyance, misinformation, loss of information and loss of money, have been seen.¹ The importance of software quality is beyond question and, hence, should be addressed seriously. Therefore, software development should always be accompanied by testing, which is a primary means to detect software failures and to prevent faults from propagating through to the final production system, where the cost of removal is far greater.

Among the research work on testing, many focus on test-case generation. This is because the comprehensiveness of test cases will affect the scope of testing and, in turn, the chance of uncovering software failures. Because of the importance of test cases, people who are in charge of performing (e.g., software practitioners) or reviewing (e.g., IT auditors) software testing activities should have a good understanding of the fundamental concepts and problems associated with test-case generation.

Fundamental Concepts of Black Box Testing

The black box approach is a mainstream type of technique for test-case generation. In this approach, test cases are generated according to information derived from the specification document (or simply the specification) without requiring the knowledge of how the programs are written. Thus, the black box approach can be applied to test off-the-shelf software packages, where the source codes are normally not available from vendors. This testing approach is very popular in the commercial sector.

There are a large variety of test-case generation methods in the black box approach, including the choice relation framework,² the classification-tree methodology,³ domain testing⁴ and orthogonal arrays.⁵ Most of these methods generate test cases in three steps:

1. Identify categories and choices from the specification.
2. Select valid combinations of choices.
3. Construct test cases from the valid choice combinations.

Example 1 illustrates these three steps.

Example 1

The example used here is a course enrollment system at a university. To evaluate whether a course enrollment by a student should be approved, the system accepts the following

inputs regarding the students concerned (Each of the following inputs will affect the functions of the system. The details, however, are not included here.):

- Student ID: A five-digit number
- Degree level: "Undergraduate" or "Postgraduate"
- Degree type: "Coursework" or "Research." All undergraduate degrees are by coursework, while postgraduate degrees can be by coursework or research.
- Degree: Examples are "BA," "BS," "BEng," "MBA" and "PhD."
- Number of courses enrolled (N): " $N = 0$," " $1 \leq N \leq 8$ " or " $N \geq 9$ "

(Step 1) First, categories are identified from the specification of the course enrollment system. A category is defined as a major characteristic of a system input or state that affects its execution behavior. Degree level, degree type and number of courses enrolled (N) are three possible categories for the course enrollment system. Second, associated choices for each category are identified. Each choice is a single value or a range of values. For example, the choices associated with the category degree level are Undergraduate and Postgraduate, while the choices associated with the category number of courses enrolled (N) are $N = 0$, $1 \leq N \leq 8$, and $N \geq 9$.

(Step 2) The term "test frame" is used here to refer to a group (or combination) of choices. If a test frame satisfies both of the following conditions—it contains a sufficient number of choices and the combination of such choices is valid—then the test frame is said to be complete; otherwise, the test frame is incomplete. Consider, for instance, the following three examples of test frames:⁶

- Test frame B_1 : { |5-digit Student ID|, |Undergraduate|, |Coursework|, |BS|, | $N \geq 9$ | }
- Test frame B_2 : { |5-digit Student ID|, |Postgraduate|, |Coursework|, |MBA| }
- Test frame B_3 : { |5-digit Student ID|, |Postgraduate|, |Coursework|, |PhD|, | $1 \leq N \leq 8$ | }

B_1 is a complete test frame, because it satisfies both conditions. B_2 is an incomplete test frame, because additional information about the number of courses in which the student enrolled is needed to construct test cases (the first condition is not met). B_3 is also an incomplete test frame because the choices of coursework and Ph.D. cannot be combined together (Ph.D. is not a coursework degree) (the second condition is not met).

Only complete (not incomplete) test frames are useful for testing, and there are some techniques (such as the choice relation framework⁷ and the classification-tree methodology⁸)

developed by software researchers and practitioners to help generate complete test frames.

(Step 3) Given a complete test frame containing one or more choices, a value is randomly selected from every choice, and the combination of the selected values forms a test case. For example, the following test case can be formed from B1 in step 2:

{Student ID = 32390, Degree Level = Undergraduate, Degree Type = Coursework, Degree = BS, Number of Courses Enrolled (N) = 9}

Major Problems of Black Box Testing

The comprehensiveness of the generated test cases depends on how well the previous three steps are performed. Until now, steps 2 and 3 are well supported by a large variety of approaches and methods developed by software researchers and practitioners. On the other hand, not much has been developed to help software testers identify categories and choices in step 1, especially for those specifications that are written mainly in narrative languages. Thus, the identification of categories and choices is often performed in an *ad hoc*, impromptu manner. Such a practice is unacceptable because the comprehensiveness of the identified categories and choices cannot be ascertained by an *ad hoc* approach. If, for example, the software tester fails to identify a valid choice, then any software fault associated with this choice may go undetected.

Example 1 seems to suggest that identifying categories and choices is a straightforward task. However, this identification exercise is not trivial for commercial specifications, which are often complex. Software testers are likely to make mistakes in an *ad hoc* identification exercise. The authors have performed three empirical studies to verify this conjecture.

Setting of Studies

Three empirical studies have been conducted to find out the common mistakes made by software testers during an *ad hoc*, impromptu identification of categories and choices from three commercial specifications. The respective specifications used in the three studies are denoted by SPEC-1, SPEC-2 and SPEC-3. The first specification, SPEC-1, is related to the credit sales of goods by a wholesaler to retail customers. SPEC-2 is related to the purchase of goods using credit cards issued by an international bank. SPEC-3 is related to an airline catering system.

More than 40 subjects were recruited for the studies. These subjects were undergraduates or postgraduates in the computer science, software engineering and IT programs at a number of universities. For each specification, every subject was asked to identify a set of categories and choices using an *ad hoc* identification approach. In addition, for every identified category or choice, the subjects were asked to state the reason of its identification to facilitate the subsequent analysis.

Types of Mistake

Before discussing the results of these studies, some important concepts must be introduced. As mentioned earlier, categories are defined as the major characteristics of system inputs or states that affect the execution behavior of a system.

For every category proposed by the subjects, it may either be identified in accordance with the definition, or incorrectly identified with something else in mind. In view of this situation, any category identified by the subjects is referred to as a potential category. Similarly, any choice identified by the subjects is called a potential choice.

In the study, it was observed that the subjects made various mistakes. The following examples illustrate these mistakes (all these examples refer to the course enrollment system in example 1):

- **Relevant and irrelevant categories**—Suppose two potential categories, namely degree level and student age, are identified by the subject. Degree level is a relevant category (or simply a category), because it is identified with respect to an input that affects the execution behavior of the system. On the other hand, student age is an irrelevant category, because the specification for the system indicates that the age of a student is not relevant to course enrollments.
- **Missing category**—Consider again the degree level category. If the subject fails to identify this category, then degree level is a *missing category*.
- **Valid and invalid choices**—Suppose a subject has identified diploma and undergraduate as two potential choices for the category degree level. Here, diploma is an invalid choice, because a diploma is not a degree program (in this case, degree level is a category with an invalid choice). On the other hand, undergraduate is a valid choice, because undergraduate and postgraduate are the two possible levels of a degree.
- **Missing choice**—Consider the number of courses enrolled (N) category. Suppose the subjects have identified only $N = 0$ and $1 \leq N \leq 8$ as the valid choices, and the valid choice $N \geq 9$ has not been identified. Then, $N \geq 9$ is a missing choice and number of courses enrolled (N) is a category with a missing choice.
- **Overlapping choices**—Suppose the number of courses enrolled (N) category is now identified with three associated choices: $N = 0$, $1 \leq N \leq 9$, and $N \geq 9$. In this case, $1 \leq N \leq 9$ and $N \geq 9$ are overlapping choices, because the value “ $N = 9$ ” exists in both choices. Number of courses enrolled (N) is a category with overlapping choices.
- **Combinable choices**—Consider the valid choice $1 \leq N \leq 8$ in the number of courses enrolled (N) category. Suppose that this choice is now replaced by two other valid choices: $1 \leq N \leq 4$ and $5 \leq N \leq 8$. Suppose it is also known that, according to the specification, the course enrollment system will behave “similarly” for any value N such that $1 \leq N \leq 8$. With this knowledge, there is no need to identify the choices: $1 \leq N \leq 4$ and $5 \leq N \leq 8$. (In this case, $1 \leq N \leq 4$ and $5 \leq N \leq 8$ are combinable choices, and number of courses enrolled [N] is a category with combinable choices.) Rather, both choices should be combined to form one single choice: $1 \leq N \leq 8$. Note that such a combination will reduce the number of complete test frames (and also test cases) subsequently generated and, hence, save testing effort. At the same time, the combination will not affect the comprehensiveness of the generated test cases.

- **Composite choice**—Suppose the number of courses enrolled (N) category is now identified with only two valid choices, $0 \leq N \leq 8$ and $N \geq 9$. Here, $0 \leq N \leq 8$ is a composite choice, because the specification states that the course enrollment system will behave “differently” with respect to $N = 0$ and $1 \leq N \leq 8$. In this case, number of courses enrolled (N) is a category with a composite choice. The composite choice, $0 \leq N \leq 8$, needs to be replaced by the valid choices, $N = 0$ and $1 \leq N \leq 8$. Otherwise, sufficient complete test frames (and, in turn, test cases) cannot be generated to test every functional behavior of the system.
- **Problematic choice**—A potential choice x in a category is said to be problematic if at least one of the following criteria is met:
 - x is an invalid choice.
 - x is one of the overlapping choices.
 - x is one of the combinable choices.
 - x is a composite choice.
- **Problematic category**—A potential category X is said to be problematic if at least one of the following criteria is met:
 - X is an irrelevant category.
 - X is a category with missing choices.
 - X is a category with problematic choices.

Note that a problematic category may satisfy more than one criterion as listed previously.

- **Problematic set of potential categories and potential choices**—Given a set (denoted by PC) of potential categories and their associated potential choices, it is said to be problematic if at least one of the following criteria is met:
 - PC has missing categories.
 - PC has problematic categories.

Results of Studies

Figure 1 shows the statistics of the potential categories (data not enclosed in parentheses) and potential choices (data enclosed in parentheses) identified for each specification. The numbers of potential categories and potential choices increased

with the complexity of the specification, with SPEC-1 being the least complex and SPEC-3 the most complex. These numbers varied substantially among the subjects, as evidenced by the large ranges and standard derivations of the numbers of potential categories and potential choices identified. This suggests that the quality of PCs, identified by the subjects in an *ad hoc* manner, also varied significantly.

Figure 2 shows the statistics of missing and problematic categories for each specification. Similar to the numbers of potential categories and potential choices shown in figure 1, the average numbers of missing categories and problematic categories in each PC also increased with the complexity of the specification. Figure 2 also shows that the percentages of PCs with missing categories and/or problematic categories in all three specifications were generally high. Two conclusions can be drawn from this latter observation. First, the occurrence of missing categories in PCs would mean that the PCs are not comprehensive, because they do not contain sufficient relevant categories (and associated valid choices) to generate enough complete test frames for testing. Second, the occurrence of problematic categories in PCs would mean that the PCs are not effective, because these problematic categories would result in the generation of incomplete test frames.

The following is some further analysis of the problematic categories identified by the subjects. Figures 3 and 4 show the percentages of different types of problematic categories,

Figure 1—Statistics of Potential Categories and Potential Choices

Specification	Number of Potential Categories (Choices)		
	Mean*	Range*	Standard Derivation
SPEC-1	5.5 (12.1)	4-9 (10-20)	0.9 (1.5)
SPEC-2	9.9 (23.7)	6-14 (15-35)	2.0 (4.4)
SPEC-3	14.0 (33.8)	4-40 (10-83)	7.8 (16.7)
* By each subject			

Figure 2—Statistics of Missing and Problematic Categories

Specification	Percentage of PCs With Missing Categories	Average Number of Missing Categories in Each PC	Percentage of PCs With Problematic Categories	Average Number of Problematic Categories in Each PC
SPEC-1	2.1%	0.02	87.5%	0.90
SPEC-2	47.9%	0.69	95.8%	1.65
SPEC-3	100.0%	3.59	93.2%	3.59

Figure 3—Percentages of Different Types of Problematic Category in All Potential Categories

Specification	Irrelevant Categories	Categories With Missing Choices	Categories With Invalid Choices	Categories With Overlapping Choices	Categories With Combinable Choices	Categories With Composite Choices
SPEC-1	0.0%	1.1%	0.0%	2.3%	0.0%	12.8%
SPEC-2	0.0%	1.9%	0.4%	5.5%	0.0%	8.8%
SPEC-3	20.0%	2.0%	2.3%	0.7%	0.8%	0.7%
Averages	6.7%	1.7%	0.9%	2.8%	0.3%	7.4%

Figure 4—Percentages of Different Types of Problematic Category in All Problematic Categories

Specification	Irrelevant Categories	Categories With Missing Choices	Categories With Invalid Choices	Categories With Overlapping Choices	Categories With Combinable Choices	Categories With Composite Choices
SPEC-1	0.0%	7.0%	0.0%	14.0%	0.0%	79.1%
SPEC-2	0.0%	11.4%	2.5%	32.9%	0.0%	53.2%
SPEC-3	77.8%	7.6%	8.9%	2.5%	3.2%	2.5%
Averages	25.9%	8.7%	3.8%	16.5%	1.1%	44.9%

Figure 5—Percentages of PCs Containing Different Types of Problematic Categories

Specification	Irrelevant Categories	Categories With Missing Choices	Categories With Invalid Choices	Categories With Overlapping Choices	Categories With Combinable Choices	Categories With Composite Choices
SPEC-1	0.0%	6.3%	0.0%	12.5%	0.0%	70.8%
SPEC-2	0.0%	16.7%	4.2%	52.1%	0.0%	64.6%
SPEC-3	75.0%	15.9%	25.0%	9.1%	6.8%	9.1%
Averages	25.0%	13.0%	9.7%	24.6%	2.3%	48.2%

in all “potential” categories and in all “problematic” categories, respectively. **Figure 5** shows the percentages of PCs containing different types of problematic categories. Furthermore, a closer examination reveals that about 88 percent, 96 percent and 93 percent of the PCs for SPEC-1, SPEC-2 and SPEC-3, respectively, contained at least one problematic category. When comparing **figures 3, 4 and 5**, the following was observed:

- The relative frequency distributions of different types of problematic category are fairly similar across all three studies.
- Categories with composite choices are the most common, while categories with combinable choices are the least common.

Conclusion

The observations during this study clearly show that the *ad hoc* identification approach in step 1 of most black box test-case generation methods is ineffective. This is because the set of potential categories and potential choices identified by a software tester under this approach is likely to be problematic. Thus, the resulting test cases generated are not comprehensive to test every functional behavior of the system. Those software developers, end users and IT auditors responsible for performing or reviewing testing activities (e.g., user acceptance tests) should be aware of this problem and its adverse impact on the comprehensiveness of testing.

The occurrence of many problematic categories and choices also indicates that there is a strong need for the development of some systematic methods for identifying relevant categories and valid choices from specifications. As an interim solution, based on the above observations, the following checklist was formulated to help software testers detect the existence of missing categories, problematic categories and problematic choices:

- For every potential category, check whether it corresponds to a system input or state that affects the execution behavior of the system being tested. If not, this potential category is irrelevant and, hence, should be ignored.

- Check whether all inputs and states affecting the execution behavior of the system have been identified as categories. If not, there are missing categories that were not identified.
- For every potential choice, check whether it does not exist in any complete test frame. If yes, this choice is invalid.
- For every category, check whether all its associated valid choices together cover all the possible values associated with this category. If not, the category contains missing choices yet to be identified.
- For every pair of valid choices in every category, determine whether these choices are overlapping by checking the existence of common values.
- When identifying potential categories and potential choices, consider also the constraints among potential choices in the formation of complete test frames and the execution behavior associated with these choices. This will help detect the occurrence of combinable choices and composite choices.

References

Hoffman, D.M.; P.A. Strooper; L. White; “Boundary Values and Automated Component Testing,” *Software Testing, Verification and Reliability*, vol. 9, no. 1, 1999, p. 3–26

Endnotes

- ¹ Grottke, M.; K.S. Trivedi; “Fighting Bugs: Remove, Retry, Replicate, and Rejuvenate,” *IEEE Computer*, vol. 40, no. 2, 2007, p. 107–109
- ² T.Y. Chen; P.-L. Poon; T.H. Tse; “A Choice Relation Framework for Supporting Category-Partition Test Case Generation,” *IEEE Transactions on Software Engineering*, vol. 29, no. 7, 2003, p. 577–593
- ³ T.Y. Chen; P.-L. Poon; T.H. Tse; “An Integrated Classification-tree Methodology for Test Case Generation,” *International Journal of Software Engineering and Knowledge Engineering*, vol. 10, no. 6, 2000, p. 647–679.
Grochtmann, M.; K. Grimm; “Classification Trees for Partition Testing,” *Software Testing, Verification and Reliability*, vol. 3, no. 2, 1993, p. 63–82.

- ⁴ Beizer, B.; *Software Testing Techniques*, Van Nostrand Reinhold, USA, 1990
- ⁵ Krishnan, R.; S.M. Krishna; P.S. Nandhan; "Combinatorial Testing: Learnings From Our Experience," *ACM SIGSOFT Software Engineering Notes*, vol. 32, no. 3, 2007, p. 1–8
- ⁶ In this list, for ease of discussion, categories are enclosed by { } and choices are enclosed by vertical bars | |.
- ⁷ *Op cit*, Chen, Poon and Tse, 2003
- ⁸ *Op cit*, Chen, Poon and Tse, 2000; Grochtmann and Grimm

Acknowledgement

The work described in this article was partially supported by a grant from the Research Grants Council of Hong Kong (Project No. PolyU 5177 /04E).

Pak-Lok Poon, Ph.D., CISA, CSQA, MACM, MIEEE is an associate professor at the School of Accounting and Finance of The Hong Kong Polytechnic University. His research interests include software testing, requirements inspection, IT audit and control, electronic commerce, business process reengineering, and computers in education. He has been a member of the Editorial Committee of the *Information Systems Control Journal* since 2002. He was a co-recipient of the Michael Cangemi Best Book/Article Award from ISACA in 2001. Before commencing his academic career, he was the computer audit manager of an international airline company. He can be reached at afplpoon@inet.polyu.edu.hk.



LEADING THE IT GOVERNANCE COMMUNITY

GUIDANCE MATERIALS FOR IT GOVERNANCE FEATURING

COBIT® 4.1

COBIT® CONTROL PRACTICES: GUIDANCE TO ACHIEVE CONTROL OBJECTIVES FOR SUCCESSFUL IT GOVERNANCE

IT GOVERNANCE IMPLEMENTATION GUIDE: USING COBIT® AND VAL IT™

IT ASSURANCE GUIDE: USING COBIT®

Also:

COBIT® Security Baseline

COBIT® Quickstart

COBIT Online®

COBIT® Mapping Papers

Aligning COBIT® 4.1, ITIL V3 and ISO/IEC 27002 for Business Benefit



ACCESS THE LATEST COBIT CONTENT AT www.isaca.org/cobit

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, security and governance 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 organisation, an IT service provider, uses a number of open source tools. As an IT auditor, what are the risks that I should be cognisant about whilst doing an audit of our IT function? What are the risks, if any, that an organisation is exposed to, by using open source tools? I also understand that there are different types of open source licences. Can you give some background information as well, before explaining the risks and controls on open source?

I am keen to know your point of view.

A I am glad to receive such an interesting and thought-provoking question. For ordinary IT users, the open source definition is a bill of the users' rights. It lists the specific rights that a software licence must grant to its users for it to be classified as open source. IT users, including programmers, enjoy working with open source software (OSS) for many reasons including:

- The right to make and distribute changes to the original program
- The right to make and distribute copies of the program

GNU General Public License (GPL), Mozilla Public License (MPL), Berkeley Software Distribution (BSD), Artistic Licenses and X Consortium are some examples of licences that meet the requirements of Open Source Definition.

The definition of open source is a specification of criteria that a particular software licence has to meet to qualify it as OSS. Any software distributed as OSS must meet the following conditions:

- **Free redistribution**—The user can make any number of copies of the software and sell them or give them away, and does not need to make payment to anyone for doing this. The user can even sell it, but does not owe any royalty to anyone.
- **Inclusion of source code**—The software distributed as OSS must contain the entire source code/program and must allow distribution of it in both forms: simple source code or compiled version. If the software were to be distributed only

in compiled form, for any reason, then the access to the original source code must be made available to those who seek it by some means, e.g., the Internet, at no charge.

- **No discrimination against anyone or any particular endeavour**—The licence must not discriminate against any individual or group of people in terms of them being recipients or not. Equally, it cannot restrict the use of the software for use in any particular field. For example, the licensor cannot prohibit the use of software for, say, research on genetics.
 - **Integrity of the authors' source code**—Some software authors have had fears that their reputation will be at risk should a modified version of the original software be distributed with some unacceptable bugs. Therefore, the OSS may restrict the distribution of the modified source codes, if and only if the licence permits the distribution of 'patch files' with the source code, for the purpose of modifying the original program at build time. Equally, the licence must allow for modifications and derived works and must allow the distribution of the derived works to be distributed under the same terms.
 - **Licence must not be product-specific**—The rights attached to the product distributed as OSS must not be interlinked with another particular piece of software. This means that a particular piece of software distributed as OSS cannot be distributed free if used with a particular brand of a particular operating system's software.
 - **Distribution of licence**—The rights attached to the OSS must apply to all users to whom the particular software is redistributed without need for execution of any additional licence by those parties. The licence must be automatic with no requirement of signature.
 - **No contamination of other software licences allowed**—The OSS must not place any restrictions on other software that is distributed along with the licensed software.
- With this background, let us discuss the risks and related controls. Whilst you have stated that your employer is an IT service provider, I am not clear on what types of service get

delivered by them. Hence, I shall try to illustrate some generic risks for your consideration:

- Any service that the enterprise chooses to provide using an OSS must abide by the previously mentioned principles and must not contravene them in any form, even partially.
- Should an OSS be used in any deliverable to a client—in some embedded form—then such use must be fully disclosed to the client. The client organisation must be made aware of any potential risks so that it can make an informed decision. If the client had prohibited the usage of any OSS for delivering any service to them, then such stipulations must be followed.
- For all purposes, the enterprise must treat any OSS as a third-party software. Any OSS comes with its own set of stipulations and requirements. Just because it comes free of cost does not mean that there are no restrictions in terms of use.

- A prudent approach is not to provide any warranty/guarantee to, or aim to indemnify, clients with respect to the use/functioning of the OSS embedded within a solution the enterprise provides, for which the enterprise will naturally provide some form of indemnity or warranty.
- The enterprise may wish to evaluate the risks of its employees participating in open source community discussions and also in terms of any product enhancements. How far such discussions benefit the enterprise or whether they cause potential damage is something that the enterprise needs to evaluate, assess and upon which make an informed decision.

Figure 1 presents some types of open source licences and their typical features. Please note that the list is not exhaustive. (There are other types, such as Artistic License, MPL, NPL and LGPL, that have not been explained in this column.)

Figure 1—Types of Open Source Licences and Their Features

Type of Open Source Licence	Explanation	Right to Interlink/Mix With Commercial Software	Right to Re-license to Any Third Party	Prevalence of Special Privileges to the Original Author Over Modifications by Third Parties
GPL	Anyone can copy and distribute any number of copies, but no one is allowed to change the original software.	No	No	No
BSD	These licences permit users to do almost anything with it. In addition, BSDs require users to mention that it was developed at the University of California.	Yes	No	No
Public Domain	A Public Domain program is one where the author has relinquished his/her rights in terms of 'copyright'.	Yes	Yes	No

Call for Articles

for *CoBIT® Focus*

CoBIT® Focus is the
CoBIT-based electronic newsletter.

For more information contact
Jennifer Hajigeorgiou at publication@isaca.org

The next issue accepting articles is January 2009.
Submission deadline is 11 December 2008.



CPE Quiz

Quiz #121

Based on Volume 4, 2008—Risk

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

Prepared by Kamal Khan, CISA, CISSP, MBCS

True or False

Tanampasidis Article

1. The new legal and ethical dilemmas and challenges to banks and their customers include impersonal communication between the bank and the customer and sensitive data interchange through public networks.
2. The Value at Risk (VaR) methodology translates the level of risk into monetary units without the need for extensive historical data.
3. One of the advantages of the VaR methodology is that the auditor focuses on the quantitative parameters of risk exposure.
4. The suggested methodology consists of six stages including strategy analysis and evaluation.
5. At the end of the third stage, identification of points of risk mitigation and control, the auditor must be in a position to identify for further investigation the residual risk.
6. The methodology described can be applied by an average-to-experienced auditor.

Ramirez Article

7. Risk management models do not contribute anything to the bottom line of the organization.
8. The AIRMIC standard includes references to areas such as risk assessment and risk analysis.
9. The COSO model includes areas recommended by other risk management models as well as a three-dimensional matrix.

Godfrey Article

10. Using Integration Protocol (IP) network architecture as a backbone, converged security solutions can add a layer of “integration intelligence.”
11. Workflow application software, embedded into the security management process, will play an important role in driving the adoption of security convergence and holistic risk mitigation.

Help Article

12. Business and IT should work on achieving their own, different objectives.
13. In COSO ERM the internal environment is the first layer, but in Pension-Fennia’s model, it was the result of the evaluation of the first six layers.
14. In the second part in every layer, the maturity of controls is evaluated with the help of different criteria.
15. The tool developed also deepened the synergy and mutual understanding between business units and IT.

Aras, Ciaramitaro, Livermore Article

16. The Gartner Group reports that more than 50 percent of current business security vulnerabilities are found within software applications rather than the network boundaries.
17. According to the American Society for Quality Control, best practices are determined through continuously identifying, understanding and adapting outstanding practices and processes found inside and outside of organizations.
18. Two best practices within code construction are secure software checklists and software inspections.

Information Systems Control Journal
CPE Quiz
Based on Volume 4, 2008—Risk

Quiz #121 Answer Form

(Please print or type)

Name _____

Address _____

CISA, CISM or CGEIT# _____

Quiz #121

True or False

Tanampasidis Article

1. _____
2. _____
3. _____
4. _____
5. _____
6. _____

Ramirez Article

7. _____
8. _____
9. _____

Godfrey Article

10. _____
11. _____

Help Article

12. _____
13. _____
14. _____
15. _____

**Aras, Ciaramitaro,
Livermore Article**

16. _____
17. _____
18. _____

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

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

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

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

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



**Narrow your search,
expand your choices.**



To explore the
Career Centre, please visit
www.isacaorg/careercentre

MEMBERSHIP APPLICATION

Join online and save US \$20.00

www.isaca.org/join

Please complete both sides

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

www.isaca.org

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 _____

AREA/COUNTRY CODE AND NUMBER

Residence facsimile _____

AREA/COUNTRY CODE AND NUMBER

Company name _____

Title _____

Business address _____

STREET

CITY

STATE/PROVINCE/COUNTRY

POSTAL CODE/ZIP

Business phone _____

AREA/COUNTRY CODE AND NUMBER

Business facsimile _____

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 Control Journal 9 ☐ Educational Event
5 ☐ Other Publication

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 Headquarters. 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 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 ☐ IT Audit Director/Manager/Consultant
8 ☐ Security Director/Manager/Consultant
9 ☐ IT Director/Manager/Consultant
10 ☐ Compliance/Risk/Privacy Director/Manager/Consultant
11 ☐ IT Senior Auditor (External/Internal)
12 ☐ IT Auditor (External/Internal Staff)
13 ☐ Non-IT Auditor (External/Internal)
14 ☐ Security Staff
15 ☐ 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

* 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).

Full payment entitles new members to membership from the date payment is processed by International Headquarters through 31 December 2009. 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 2008 through 31 May 2009.

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, or contact your local chapter at www.isaca.org/chapters.

Chapter Name	Chapter Number	Dues
ASIA		
Hong Kong	64	\$60
Bangalore, India	138	\$20
Cochin, India	176	\$15
Coimbatore, India	155	\$20
Hyderabad, India	164	\$20
Kolkata, India	165	\$20
Chennai, India	99	\$10
Mumbai, India	145	\$35
New Delhi, India	140	\$15
Pune, India	159	\$17
Vijayawada, India	200	\$20
Indonesia	123	\$45
Nagoya, Japan	118	\$60
Osaka, Japan	103	\$85
Tokyo, Japan	89	\$80
Korea	107	\$40
Lebanon	181	\$35
Macao	190	\$0
Malaysia	93	\$10
Muscat, Oman	168	\$40
Karachi, Pakistan	148	\$20
Lahore, Pakistan	196	\$30
Manila, Philippines	136	\$20
Jeddah, Saudi Arabia	163	\$70
Riyadh, Saudi Arabia	154	\$0
Singapore	70	\$10
Sri Lanka	141	\$15
Taiwan	142	\$50
Bangkok, Thailand	109	\$10
UAE	150	\$10

CENTRAL/SOUTH AMERICA

Buenos Aires, Argentina	124	*
Mendoza, Argentina	144	*
LaPaz, Bolivia	173	\$25
São Paulo, Brazil	166	\$20
Santiago, Chile	135	\$40
Bogotá, Colombia	126	\$25
San José, Costa Rica	31	\$33
Quito, Ecuador	179	\$15
Guadalajara, México	201	\$40
Mérida, Yucatán, México	101	\$50
Mexico City, México	14	\$65
Monterrey, México	80	\$50
Panamá	94	\$30
Asunción, Paraguay	184	\$40

Lima, Perú	146	\$15
Puerto Rico	86	\$40
Montevideo, Uruguay	133	*
Venezuela	113	\$20

EUROPE/AFRICA

Austria	157	\$45
Belgium	143	\$70
Sofia, Bulgaria	189	\$40
Croatia	170	\$50
Czech Republic	153	\$130
Denmark	96	\$50
Estonia	162	\$30
Finland	115	\$15

Chapter Name	Chapter Number	Dues
France (Paris)	75	\$140
Germany	104	\$80
Athens, Greece	134	\$30
Budapest, Hungary	125	\$65
Ireland	156	\$40
Tel-Aviv, Israel	40	\$50
Milan, Italy	43	\$53
Rome, Italy	178	\$26
Kenya	158	\$40
Latvia	139	\$20
Lithuania	180	\$40
Luxembourg	198	\$85
Malta	186	\$25
Netherlands	97	\$50
Abuja, Nigeria	185	\$40
Lagos, Nigeria	149	\$20
Norway	74	\$55
Warsaw, Poland	151	\$40
Moscow, Russia	167	\$10
Romania	172	\$50
Slovenia	137	\$50
Slovak Republic	160	\$65
South Africa	130	\$49
Barcelona, Spain	171	\$110
Madrid, Spain	183	\$85
Valencia, Spain	182	\$45
Sweden	88	\$45
Switzerland	116	\$45
Tanzania	174	\$50
Kampala, Uganda	199	\$0
London, UK	60	\$40
Central UK	132	\$55
Northern England, UK	111	\$75
Scotland, UK	175	\$80

NORTH AMERICA

Canada

Calgary, AB	121	\$25
Edmonton, AB	131	\$25
Vancouver, BC	25	\$20
Victoria, BC	100	\$0
Winnipeg, MB	72	\$20
Nova Scotia	105	\$0
Ottawa Valley, ON	32	\$16
Toronto, ON	21	\$25
Montreal, PQ	36	\$25
Quebec City, PQ	91	\$45

Islands

Bermuda	147	\$0
Trinidad & Tobago	106	\$25

Midwestern United States

Chicago, IL	02	\$50
Illini (Springfield, IL)	77	\$30
Central Indiana (Indianapolis)	56	\$30
Michiana (South Bend, IN)	127	\$0
Iowa (Des Moines)	110	\$25
Kentuckiana (Louisville, KY)	37	\$35
Detroit, MI	08	\$40
Western Michigan	38	\$30
Minnesota	07	\$35
Omaha, NE	23	\$30

Chapter Name	Chapter Number	Dues
Central Ohio (Columbus)	27	\$35
Greater Cincinnati, OH	03	\$30
Northeast Ohio (Cleveland)	26	\$30
Northwest Ohio	188	\$25
Kettle Moraine, WI (Milwaukee)	57	\$35
Quad Cities	169	\$25

Northeastern United States

Greater Hartford, CT	28	\$40
Central Maryland (Baltimore)	24	\$25
New England	18	\$30
New Jersey	30	\$40
Central New York (Syracuse)	29	\$15
Hudson Valley, NY (Albany)	120	\$0

New York Metropolitan	10	\$50
Western New York (Buffalo)	46	\$30

Harrisburg, PA	45	\$25
Philadelphia, PA	06	\$40
Pittsburgh, PA	13	\$20
Rhode Island	197	\$25
National Capital Area, DC	05	\$40

Southeastern United States

North Alabama (Birmingham)	65	\$30
Jacksonville, FL	58	\$30
Central Florida (Orlando)	67	\$35

South Florida	33	\$40
West Florida (Tampa)	41	\$35
Atlanta, GA	39	\$40
Charlotte, NC	51	\$35
Research Triangle (Raleigh, NC)	59	\$25
South Carolina Midlands (Columbia, SC)	54	\$30
Memphis, TN	48	\$45
Middle Tennessee (Nashville)	102	\$45
Virginia	22	\$30

Southwestern United States

Central Arkansas (Little Rock)	82	\$60
Denver, CO	16	\$40
Baton Rouge, LA	85	\$25
Greater New Orleans, LA	61	\$25
Greater Kansas City, MO	87	\$0
St. Louis, MO	11	\$25
New Mexico (Albuquerque)	83	\$25
Central Oklahoma (OK City)	49	\$30
Tulsa, OK	34	\$30
Austin, TX	20	\$25
Greater Houston Area, TX	09	\$40
North Texas (Dallas)	12	\$30
San Antonio/So. Texas	81	\$25

Western United States

Anchorage, AK	177	\$20
Phoenix, AZ	53	\$30

Chapter Name	Chapter Number	Dues
Los Angeles, CA	01	\$25
Orange County, CA (Anaheim)	79	\$30
Sacramento, CA	76	\$25
San Francisco, CA	15	\$45
San Diego, CA	19	\$40
Silicon Valley, CA (Sunnyvale)	62	\$30
Hawaii (Honolulu)	71	\$40
Boise, ID	42	\$40
Las Vegas, NV	187	\$35
Willamette Valley, OR (Portland)	50	\$30
Utah (Salt Lake City)	04	\$30
Mt. Rainier, WA (Olympia)	129	\$20
Puget Sound, WA (Seattle)	35	\$25

OCEANIA

Adelaide, Australia	68	\$0
Brisbane, Australia	44	\$16
Canberra, Australia	92	\$15
Melbourne, Australia	47	\$15
Perth, Australia	63	\$10
Sydney, Australia	17	\$30
Auckland, New Zealand	84	\$40
Wellington, New Zealand	73	\$28
Papua New Guinea	152	\$10

To receive your copy of the *Information Systems Control Journal*, please complete the following subscriber information:

Size of ENTIRE organization

- ① ☐ Fewer than 50 employees
 ② ☐ 50 – 149 employees
 ③ ☐ 150 – 499 employees
 ④ ☐ 500 – 1,499 employees
 ⑤ ☐ 1,500 – 4,999 employees
 ⑥ ☐ 5,000 – 9,999 employees
 ⑦ ☐ 10,000 – 14,999 employees
 ⑧ ☐ 15,000 or more employees

Size of IT audit staff (local office)

- ① ☐ 0 individuals
 ② ☐ 1 individual
 ③ ☐ 2-5 individuals
 ④ ☐ 6-10 individuals
 ⑤ ☐ 11-25 individuals
 ⑥ ☐ More than 25 individuals

Size of information security staff (local office)

- ① ☐ 0 individuals
 ② ☐ 1 individual
 ③ ☐ 2-5 individuals
 ④ ☐ 6-10 individuals
 ⑤ ☐ 11-25 individuals
 ⑥ ☐ More than 25 individuals

Your level of purchasing authority

- ① ☐ Recommend products/services
 ② ☐ Approve purchase
 ③ ☐ Recommend and approve purchase

ALLIED SEARCH, INC.

Professional and Executive Search

Nationwide - All States

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

MAILING ADDRESS

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

OPPORTUNITIES NATIONWIDE

POSITIONS:

IT Audit positions and other positions that prefer IT Audit experience.

LEVELS:

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

CLIENTS:

Large companies in most 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 IT Audit experience is 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 (Microsoft Word formatted)

Fax: 415-921-5309 Attn.: Don May, Managing Director

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.

Advertisers/Web Sites

ACL	www.acl.com/ISACAJournal	4
Allied Search*	www.alliedsearchinc.com	63
Caseware Idea Inc.	www.caseware-idea.com/smartanalyzer	1
CCH Teammate	www.CCHGroup.com/ISJ	Inside Back Cover
Computer Associates	www.ca.com/solutions/infogov	Back Cover
Cyber-Ark	www.cyber-ark.com/ISACA108	8
Data Blueprint	www.datablueprint.com	32
ExamMatrix	www.ExamMatrix.com/ISJ	32
Favored Solutions	www.favoredsolutions.net	29
Georgia Tech*	www.dlpe.gatech.edu/it/isad	50
Lander International LLC*	www.landerint.com	15
Modulo	www.modulo.com	10
Paisley Consulting	www.paisley.com	11
SMU*	www.EngineeringLeaders.smu.edu	29
Veridion	www.veridion.net	3
WizSoft	www.wizsoft.com	21

* 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

Media Relations

Deborah Vohasek
Kristen Kessinger
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

The YGS Group
advertising@isaca.org

Editorial Committee

Chair, Rupert Dodds, CISA, CISM, FCA
Linda Betz
Christos Dimitriadis, Ph.D., CISA, CISM
Ken Doughty, CISA, CBCP
Adam Ely, CISA
Manish Gupta, CISA, CISM, CISSP
Francisco Igual, CISA
Alan Lord, CISA, CPA
Juan Macias
David Earl Mills, CISA, MCSE
Dorcas Mutonyi
Pak-Lok Poon, Ph.D., CISA, CSQA, MIEEE
Parvathi Ramesh, CISA, CA
Carlos Villamizar Rodriguez, CISA
B. Ganapathi Subramaniam, CISA, CIA, CISSP, SSCP, CCNA, CCSA, BS 7799 LA
Aureo Monteiro Tavares Da Silva, CISM

ISACA Board of Directors (2008-2009):

International President
Lynn Lawton, CISA, FBSC CITP, FCA, FIIA, PIIA

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

Vice President
Yonosuke Harada, CISA, CISM, CAIS

Vice President
Howard Nicholson, CISA, CGEIT

Vice President
Jose Angel Pena Ibarra, CGEIT

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, 2005-2007
Everett C. Johnson Jr., CPA

Past International President, 2003-2005
Marios Damianides, CISA, CISM, CA, CPA

Director
Greg Grocholski, CISA

Director
Tony Hayes

Director
Jo Stewart-Rattray, CISA, CISM, CSEPS

Chief Executive Officer
Susan M. Caldwell