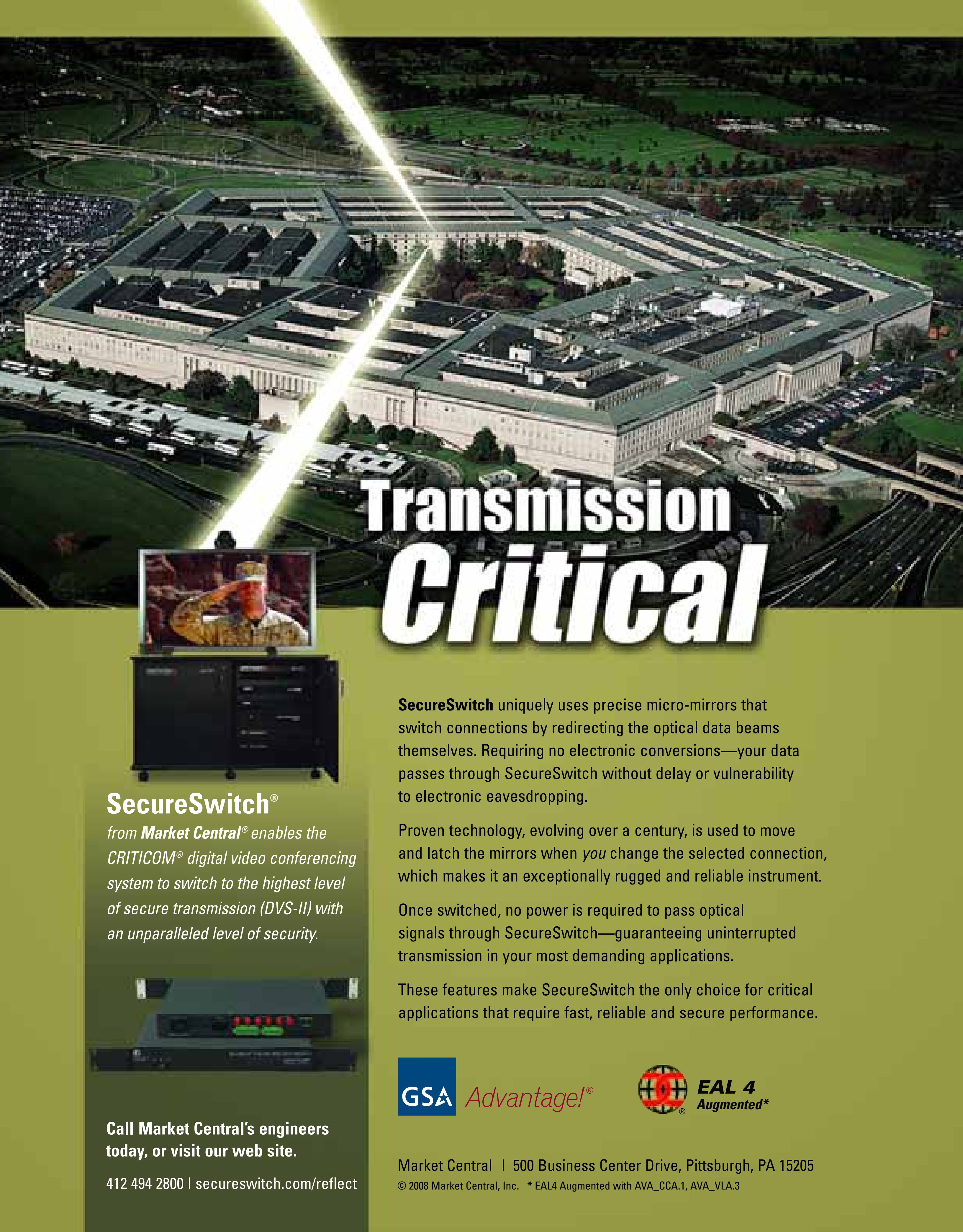


Information Systems Control JOURNAL

The Magazine for IT Governance Professionals

VOLUME 5, 2008

Columns

Features

Plus

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.

ISACA®
Serving IT Governance Professionals

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.

JOnline

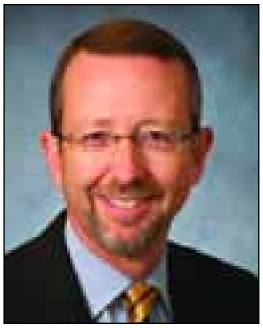
Want more of the practical, peer-reviewed articles you have come to expect from the *Journal*? Additional online-only articles will be available on the first business day of each month in which no *Journal* is released, including February, April, June, August, October and December. These articles will 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***.

Online Features

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

IDEA

Chief Audit Executive
Technical Audit Specialist
Internal Auditor
Audit Team Manager



Bob Kress is the senior director of business operations for Accenture's internal IT organization. He can be reached at *robert.e.kress@ accenture.com*.

Guest Editorial

Industry leaders examine the latest business issues

Running IT as a Business:

IT Metrics Propel Transformation

Successful IT leaders understand that IT serves the business. Performance measurement, metrics and reporting are as important to IT as they are to any business. Routine, critical evaluation of initiatives, coupled with expert management, can transform the IT organization into a strategic asset.

By measuring and tracking IT performance, organizations can make better technology investment decisions and benchmark IT against industry peers. Moreover, an objective assessment of IT capabilities can be used to inform and persuade clients, business leaders and end users.

IT transformation is about more than technological innovation; it is about innovation that brings real business value to organizations. It improves decision making, eliminates redundancies and saves money. As a partner to business, IT should maximize the power of a company's investments and minimize related operational expenses.

Aligning IT processes to business goals streamlines operations. Key to IT success is the ability to measure the progress of IT initiatives against IT strategy and to communicate results in universal business terminology. Explaining IT investments using return on investment (ROI) and establishing business benefits make business leaders more accountable for technology investments.

The following are four important tips every organization should consider for measuring and tracking IT performance.

Take a Managed Services Approach

A switch from a one-size-fits-all model of IT management (e.g., costs are centrally located, products and services are not defined, and service levels are lacking) to a strategic approach provides an ability to customize IT products and services to the business needs. By defining a set of products and services for the business with service-level guarantees and prices that are benchmarked to the marketplace, organizations can realize substantial cost savings and maintain—and often enhance—service levels.

Track Progress

Basic IT metrics such as costs, progress on key initiatives and service uptime are important, but an IT scorecard (see **figure 1**) that measures progress against business goals enables IT leaders to provide better context and more meaningful data with which to run the IT business.

A scorecard should measure IT contribution, IT operational excellence and best-in-class workplace by asking questions such as:

- How satisfied are employees, business sponsors (those who make the case for specific technology programs) and end users?
- Is IT achieving the benefits expected by the initial business cases?
- What is the cost of providing IT to different workforces?
- What is the training budget spent per employee?

The IT scorecard helps determine what is driving IT cost, where value is added (or not) and how to focus IT efforts.

Another valuable way to track progress is to engage an industry analyst firm to benchmark an enterprise against competitors. One should consider using IT expense as a percentage of net revenue, IT workforce as a percentage of headcount, and IT expense per employee. Tracking the gaps between customer satisfaction and improvements helps to guide IT investments, too.

Consistent metrics allow year-to-year comparisons, elucidate trends and enable documentation of where IT has added value.

Figure 1—Sample Strategic IT Performance Scorecard

IT Contribution	
Sponsor	0-5 (Max)
Employee	0-5 (Max)
Critical processes/roles	0-5 (Max)
Benefits enabled (realized business-case benefits)	% realized, $ actual to date
Market image	Market and business development contributions
IT Operational Excellence	
IT expense as percent of net revenue	%
IT expense per employee	$ per person
IT productivity/cost-effectiveness improvements	$ (△ IT expense per employee multiplied by the total headcount)
Service levels	% targets achieved
IT expense (with interest)	Quarter ending reforecast
On-time delivery of initiatives	% delivered on time
Workforce targets	#, %
Best-in-class Workplace	
Overall employee attrition (managed/unmanaged)	%
Employee attrition—top performers, unmanaged	%
Employee satisfaction	Satisfaction index %
Percent of training budget spent	%

© Accenture. All rights reserved.

Implement Governance

While most chief information officers are responsible for creating the overall IT strategy, the people who run the various parts of the company are the sponsors of IT and should be integrally involved in technology decisions.

Implementing a governance structure, such as an IT steering committee (ITSC) comprised of chief operating officers from each line of business within the organization, ensures that:

- Technology initiatives are aligned with the needs of the business
- The business supports what IT is doing

The benefit of taking a full life-cycle view, from the development of the original business case through the benefits realization process, should be considered. The business sponsor is responsible for establishing a baseline for business benefits in the business case and then reviewing the business case and benefits with the ITSC. If the business case is approved, benefits are tracked and monitored and the ITSC is kept apprised of changes to projected benefits.

For an additional layer of governance, sample IT initiatives and benefits should be randomly audited for a specific time frame, e.g., three years following project deployment. The double scrutiny makes business cases far more rigorous and ensures that the most business-focused investments move to the top of the IT priority list.

View IT As a Business

Creating a two-way dialog between IT and business leaders enables IT organizations to deliver innovative solutions and services that support customer-facing processes, creating a competitive advantage.

Conclusion

Keeping IT performance in lockstep with the business, by tracking progress against critical IT initiatives and using the resulting information to strengthen and inform IT investment decisions, allows organizations to derive enterprisewide value from their IT.

Disciplined metrics help forecast IT costs and IT budgets, while helping the total company plan for future growth, revenue and profit margins.

While there's no silver bullet, implementing IT metrics is worth the hard work. The results will speak for themselves. As Henry David Thoreau once said, "In the long run, men hit only what they aim at. Therefore, they had better aim at something high." As a business imperative in a competitive industry, the sentiment works well.

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

Cyber-Ark®

The Leader in Privileged Identity Management Solutions

PASSPORT
CISA
PASSPORT
CISM
CERTIFIED INFORMATION SECURITY MANAGER
to Success
PASSPORT
CGEIT
to Success
2008
AIRPORT, MUSCAT
STOCKHOLM
PASSPORT
VISA
CANADA

Reliable Security

By Steven J. Ross, CISA, CBCP, CISSP

There was a time in the not-so-distant past when information technology presented us with security problems for which there were no available technical countermeasures. It might frighten the children if they were to learn that there was once a time when computer viruses erupted but there was no antivirus software, when there were commercial web sites with no way to ensure the integrity of the message traffic flowing from the client to the server, when passwords flew across networks in the clear. Imagine that!

We are at an interesting juncture today; there are no threats to information technology for which we do not have the tools to combat them.[1] And yet, there seem to be no lack of information security problems yet to be resolved at the organizations I encounter. Simply put, it appears that we know what to do to achieve information security, but we are not doing it. More subtly, most organizations have achieved a certain level of information security, but security is not reliable in all instances. Can we functionally equate security most of the time with security all the time? This conundrum has been on my mind for some time, and I would like to expend a few words now considering why it is so.[2]

We know what to do to achieve information security, but we are not doing it.

Company Size

First, I would like to eliminate the answer: "Management just does not get it." There have been too many news reports of data privacy breaches, regulatory investigations and hacking incidents for anyone in management to claim ignorance of the threats related to information security. If, in fact, management in a given company is unaware of the extent of the risk to their company's information and systems, then I believe the onus is on that company's information security professionals to make the case. If a company does not have an information security function, then the information systems (IS) auditors need to make the case. And if there are no auditors, then we are dealing with an organization that is, in almost all cases I am familiar with, so small that information security as practiced at larger firms is not realistically affordable. So perhaps the first answer to the question of security reliability is that some organizations are too small to achieve more than a rudimentary level of protection, which may indeed suit their circumstances.

Human Frailty

The next answer that presents itself to my mind is simple human error, sins of both commission and omission. The sheer complexity of the systems to be protected, the enormity of the amount of data to be controlled and the extensiveness of the networks to be defended combine to make it almost impossible for mistakes not to creep in. At some point someone will be given access to something to which he/she was not supposed to have access.

This leads to a strong argument for the automation of many information security activities. Identity management and automated compliance, both discussed in this space in the past,[3] are two obvious examples where human intervention can be minimized. With automation, as an overarching statement, rules are set and then systems enforce them. However, the rules are made by the same humans whose frailty is at the root of the problem. Reliance on automation to police other automated systems is based on the assumption that we are better at understanding generalities (i.e., rules) than specifics (i.e., instances of the application of those rules), an assumption that is not always borne out. I have learned to my rue that any statement beginning with words such as all, none or every—generalities—is usually wrong. Specific statements often are easier to confirm.

Risk Management

A little-explored reason for the unreliability of information security is risk management. Of course, risk management is a powerful contributor to the efficiency and effectiveness of organizations' responses to the many and varied potential sources of harm that they all face. A basic principle of risk management is that one should determine the greatest sources of threats and vulnerabilities. These should be dealt with first, with the greatest amount of attention and resources. Implicit in that statement, however, is that those threats and vulnerabilities not identified as the most significant should be dealt with later (if later ever comes). Less attention and resources are afforded for these so-called lesser risks.

I use the term "so-called" because a risk is only a lesser one until it occurs. It may be that "in Hertford, Hereford and Hampshire hurricanes hardly happen," but that is scant consolation when the cottage roof is blown away. The risks considered to be relatively trivial in prospect rise to the top of the rank when, despite expectations, they actually transpire. In my opinion, what leads to this state of affairs is risk management decisions based on probability or, more precisely, a misreading of the term. Properly speaking, "probability" means the number of instances of a certain event over a period of time (e.g., once in 100 years). This should not be confused with “likelihood,” the rather vague sense as to whether an event will occur at all. In fact, the source of a security breach that happens infrequently does have a certain probability, small though it may be. “Rarely” does not equal “never,” although many manage as though it does.

The proper consideration is credibility rather than probability. If misuse of information assets, a hack, a virus, eavesdropping or fraud are real and credible risks, protections should be put in place to mitigate them. The failure to do so lets the little things become big ones and undermines the reliability of security.

Time Lag

A source of problems related to risk management is time lag. That is, everything cannot be done at once, hence the issues noted previously. If one considers all the technology and all the applications in a given organization, as well as the rate of change that occurs to them, the ability to manage the security of all of them all of the time approaches a mathematical impossibility. Thus, at any given time, there are some data, infrastructure or applications that are better protected than others, not because the technology is not available, but because the people in charge just have not gotten to them yet. Alternatively, they may think that they have addressed the risks, but did so a long while ago. The underlying asset may change, but the protective mechanisms do not keep up.

Readers who have gotten this far must be morose at this point. Does all of the foregoing mean that security can never, or at least will never, be reliable? In a sense, yes. Life does not come with guarantees. But there is a difference between reliability and certainty. We will never make information security unfailing, but we can make it reliable enough.

Endnotes

[1] I realize that I have stuck my neck out with this sentence, and invite readers to suggest instances in which I am wrong. So I will go a bit further and say that if such open risks exist, they are on the periphery of the work done in the business world as opposed to arcane laboratory environments.

[2] In 2004, I published an article in this *Journal* titled “Maybe We Have Won” that similarly suggested that previous challenges had been overcome. My suggestion at that time is that the change in technology had heralded an evolution of the information security function, which I still believe.

[3] “Identifier Management,” *Information Systems Control Journal*, vol. 3, 2003, and “Automating Compliance,” *Information Systems Control Journal*, vol. 5, 2007

Steven J. Ross, CISA, CBCP, CISSP
is a director at Deloitte. He welcomes comments at *stross@deloitte.com*.

Information Security Training

From knowledge to practice

ISO 27001 Training

ISO-27001
Lead Auditor

ISO 27001 Lead Auditor

The ISO 27001 Lead Auditor course provides you with the necessary knowledge to perform an audit or be in charge of ISMS (Information Security Management System) audit.

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

RAB QSA

ISO-27001
Lead Implementer

ISO 27001 Lead Implementer

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

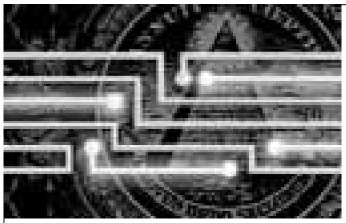
The training is also aligned with project management best practices regarding the Project Management Institute (PMI) and the International Project Management Association (IPMA) as well as the ISO 10006 standard, "Guidelines for quality management in project".

United States of America		International	
Anaheim	Las Vegas	Alger	Mexico
Atlanta	Los Angeles	Beijing	Montreal
Boston	New York	Brussels	Paris
Buffalo	San Diego	Bucharest	Prague
Chicago	San Francisco	Casablanca	Sydney
Dallas	Seattle	Geneva	Tokyo
Detroit	Tampa	Hong Kong	Toronto
Houston	Washington	Madrid	Vancouver

Veridion
From knowledge to practice

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

www.veridion.net



IT AUDIT BASICS

What Every IT Auditor Should Know About Frauds

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.*

Until the Enron and Worldcom scandals, followed by the passage of the Sarbanes-Oxley Act in July 2002, fraud education and training were sparse in the auditing profession and accounting academe. Since then, there has been an explosion of standards, training and educational offerings. But, there are still many subtleties about fraud that are not commonly known or understood, and are often critically important in fraud detection. This article will address some of the axioms about fraud that can be applied to IT audits or audits in general.

Basic Axioms of Fraud

The Association of Certified Fraud Examiners (ACFE) periodically conducts research into frauds resolved and provides statistics and information from the surveys to the public in its “Report to the Nation” (RTTN). According to the ACFE and its most recent RTTN, there are four basic axioms about fraud.

The first one seems trivial and intuitively obvious: fraud is clandestine. However, all auditors should remember this fact when performing audit procedures and in fulfilling their responsibilities to protect the public. Of course, the fraudster is being secretive and, of course, the fraud is hidden from prying eyes, as much as possible. But the important thing to remember is that if a fraud is being perpetrated, the fraudster is working hard to keep it hidden, including extra efforts to “fool” the auditor. That recognition could be interpreted as “professional skepticism.” The point is, just because audit trails and results of audit procedures appear to be proper, they could be improper because the fraudster is working hard to hide the fraud. It is also true that, just because results appear to be proper, it could be that the procedures did not select one of those transactions.

In the case of financial audit, it is true that financial audit procedures are not highly effective at detecting frauds. For instance, statistics from the 2002, 2004 and 2006 RTTNs show about 10 percent of frauds as being detected by financial audits. The 2003 KPMG Fraud Survey showed about the same percentage. Financial audit procedures are designed to detect material misstatements, not immaterial frauds!

It could also be that “red flags” of fraud were seen, but not recognized, by the auditor, because they were cleverly crafted or not recognized out of the auditor’s lack of understanding about that particular red flag (e.g., an Excel-generated invoice, missing physical address of a vendor, improper EIN). Therefore, there are many risks associated with fraud, even when there is little to no suspicion in audit procedures, because fraud is clandestine. It is critically important to auditors that if a high level of suspicion of fraud does arise, they should remember that the fraudster is working hard to hide it and further evidence. One particularly dangerous circumstance is when the auditor finds a transaction or event that is highly suspicious of fraud, but the amount is trivial and it is the only suspicious activity.

The second axiom is the fact that a fraud violates the perpetrator’s fiduciary duties to the victim organization. Many fraudsters try to structure the fraud around benign motivations or rationalizations. Fraudsters sometimes argue that no one was hurt, or that the amount of loss was extremely insignificant to the victim organization, or that the money was spent on a good cause. However, because invariably the fraudster is in a position of trust and because the fraudster violated that trust, the fact is the fraudster violated his/her fiduciary duties to the victim and, thus, there is a crime.

Third, the fraud is committed for the purpose of direct or indirect financial benefit. In the case of the latter, there have been frauds where none of the proceeds went directly to the fraudster’s benefit. For example, in one case, all of the stolen assets were spent on an animal shelter for homeless animals. In another, all stolen monies went to fund an alternative source of fuel. The interpretation in these two cases is that the fraudster benefitted indirectly.

Fourth, a fraud always costs the victim organization: assets, revenues or resources. A fraud usually results in obvious financial loss, although the calculation of the amount is sometimes complicated. Certain types of frauds may not appear to cost the organization real losses on the surface. For example, financial statement fraud is "cooking the books" and involves no real or direct theft of assets by the fraudster. However, it usually causes the victim organization to lose revenues (or stock value) once the fraud is exposed, because of the loss of the public's confidence. In fact, that rationale is one reason why managers do not want to prosecute frauds against the company (asset misappropriation or corruption) or allow them to become public knowledge. Another situation is one where an employee uses company time and computers to engage in selling objects online. This situation can be confusing or clear, depending on how fraud is defined by that entity. One definition, from the ACFE, is "the use of one's occupation for personal gain through the deliberate misuse or theft of the employing organization's resources or assets."

Using this definition, the situation of an employee selling objects online while at work clearly costs the victim organization some resources and is, thus, classified as a fraud. Obviously, an organization may choose to allow employees to specifically use company time and computers to engage in this activity, but this scenario points out the importance of a definition and the communication of it to all employees. A best practice is to publish it as part of a fraud policy, which could be incorporated into the entity's ethics policy.

Fraudster Axioms

There are some other axioms that are also generally true across frauds. These involve the fraudster.

The next axiom is one that is easily overlooked in practice. Generally speaking, white-collar criminals are individuals who have a relatively good job, have a position of trust, (usually) have a personal code of ethics (or perceive themselves to be fine human beings and law-abiding citizens) and have no criminal record. In fact, about 90 percent of the frauds committed between 2004 and 2006 were committed by someone with no criminal record, according to the 2006 RTTN. Fraudsters tend to be more educated, more tenured at the entity and well-respected. The profile of a typical fraudster leads to one obvious conclusion: they do not look like crooks. This axiom is a sober reminder of the importance of professional skepticism.

This fact leads to another axiom. Because typical fraudsters have some kind of personal code of ethics, they usually are skittish about committing the first offense. So the first offense is usually a small amount with a carefully crafted excuse, in case someone catches the instance of fraud. But, like all other criminals, it becomes easier for the fraudster to commit the subsequent offenses. It really starts when they "test the waters" and then begin to ramp up the frequency or amount. But, again, the initial instance is usually a small amount, done with some trepidation.

This leads to the next axiom of the fraudsters who get caught: they tend to escalate their crimes. Escalation could occur as frequency of the same fraud scheme, or a higher amount per instance of that fraud scheme, or adding another scheme. The greedy ones might do all three. For instance, in the 2006 RTTN, more than 4 percent of all frauds involved a financial statement fraud, a corruption fraud and an asset misappropriation fraud.

Thus, typically, fraudsters who do not get caught on the first few fraudulent transactions or events get comfortable in taking more and more money from the victim entity. It is estimated that two-thirds of frauds are never caught. It is possible that most of those fraudsters are more disciplined in their crimes.

Finally, the discovery of a small amount of fraud and/or a small number of fraudulent transactions is usually the tip of the iceberg. Fraudsters who get caught with a handful of fraudulent transactions will sometimes confess to those and declare that those were the extent of the fraud. Over and over, fraudsters have lied about the extent of their fraud. Therefore, when an auditor finds a single fraudulent transaction, or a couple of small amounts, it is not wise to assume they have discovered all of that fraud that exists, even with a confession and agreement to pay back the loss. This situation is especially true in financial audits where auditors are dealing with samples and other techniques that have limited ability to detect fraud.

Conclusion

Fraud detection is a difficult objective in any audit. The previously mentioned axioms help to explain why that is true. Taken as a whole, these axioms should empower the IT auditor to be more aware of the possibilities and characteristics of fraud, and thus be more prepared to recognize or detect fraud. If nothing else, they should raise our level of professional skepticism and help to minimize the ability of a fraudster to fool the auditor.

Pepperweed
Pepperweed Process Model
Select a process to begin your journey.
Enjoy!

STANDARDS, STATEMENTS, GUIDELINES

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

IS Auditing Procedures

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

Standards for Information System Control Professionals Effective 1 September 1999

<u>510 Statement of Scope</u>
.010 Responsibility, Authority and Accountability
<u>520 Independence</u>
.010 Professional Independence
.020 Organisational Relationship
<u>530 Professional Ethics and Standards</u>
.010 Code of Professional Ethics
.020 Due Professional Care
<u>540 Competence</u>
.010 Skills and Knowledge
.020 Continuing Professional Education
<u>550 Planning</u>
.010 Control Planning
<u>560 Performance of Work</u>
.010 Supervision
.020 Evidence
.030 Effectiveness
<u>570 Reporting</u>
.010 Periodic Reporting
<u>580 Follow-up Activities</u>
.010 Follow-up

Code of Professional Ethics Revised May 2003

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, KPMG LLP, USA
Meera Venkatesh, CISA, CISM, ACS, CISSP, CWA, Microsoft Corp., USA

Val IT Framework 2.0—Adding Breadth and Depth to the Value Management Road Map

By John Thorp, CMC, ISP

As discussed in an earlier *Journal* article,[1] all enterprises, large or small, private or public, for-profit or not-for-profit, exist to deliver value to their stakeholders, be they owners or shareholders of private companies, recipients of services from not for profits, or taxpayers. One critical challenge that enterprises face is how to ensure that they realize value from their increasingly large-scale and complex investments in information technology and IT-enabled change.

Val IT™, from the IT Governance Institute® (ITGI™), provides proven practices to help enterprises address this challenge and realize value from such investments. Val IT is applicable to all enterprises and addresses all aspects that should be contained in defining, evaluating, selecting and managing any such investment. Val IT is relevant to all management levels across both the business and IT functions—from the chief information officer (CIO) and the C-suite, to those directly involved and responsible for the selection, procurement, development, implementation, deployment and benefits-realization processes. Although primarily targeted at investments involving IT, the practices included in Val IT apply to most if not all business-change investments, whether or not involving IT.

Val IT Framework 1.0

The first edition of *The Val IT Framework* was released in February 2006. As the core publication in the Val IT series, *Enterprise Value: Governance of IT Investments, The Val IT® Framework* presented principles, processes and key management practices for three domains:

- Value Governance (VG)
- Portfolio Management (PM)
- Investment Management (IM)

This first edition was primarily targeted at new IT-enabled business investments—significant business investments in sustaining, growing or transforming the business with a critical IT component, where IT is a means to an end, the end being to contribute to the process of value creation in the enterprise.

Val IT Framework 2.0

The latest edition, *Enterprise Value: Governance of IT Investments, The Val IT® Framework 2.0*,[2] released in July 2008, aligns terminology more closely with *Control Objectives for Information and related Technology* (COBIT), and extends the Val IT framework beyond new investments to encompass all IT expenditures including ongoing IT services, assets and other resources. It adds more depth to the framework by adding management guidelines that provide greater detail on the Val IT processes and key management practices, including maturity models for each Val IT domain.

Extending the Framework

While failures of new IT investments get a lot of attention, they represent only a small percentage of overall IT expenditures. Studies show that 60-80 percent or more of IT expenditures relate to "keeping the lights on," i.e., managing the IT services resulting from previous investments such that they are delivered reliably, available when and where required, secure, and continue to contribute to business value at an affordable cost with an acceptable level of risk.

The Val IT Framework 2.0 extends the scope of Val IT to all IT expenditures by:

- Restructuring and extending the VG processes to include a broader range of operational IT portfolios, such as IT services, assets and other resources that might be added to as a result of investments managed by Val IT, but that would be managed by COBIT, with performance of those portfolios being reported back to Val IT
- Including more explicit links to COBIT in the IM processes related to populating and monitoring the performance of IT operational portfolios

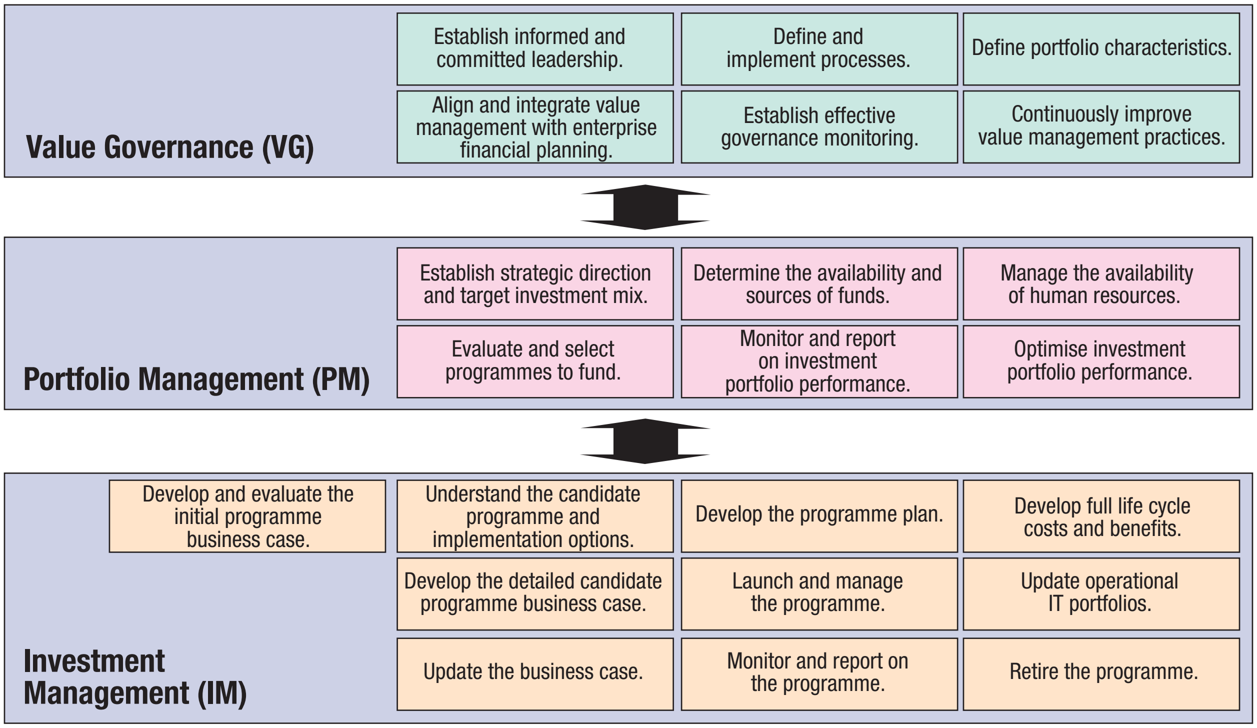
The PM processes have also been restructured and refocused to be specifically related to the investment portfolio.

The high-level interrelationships between the *The Val IT Framework 2.0* domains and processes are illustrated in **figure 1**.

The updating of the Val IT framework has significantly enhanced the key management practices within it. These enhancements provide more emphasis and focus on:

- Understanding and communicating what constitutes value to an enterprise. Without such an understanding, there is little basis for selecting investments or determining if they are contributing value.
- The opportunity for IT to influence, not simply support, business strategy. Traditionally, IT has been considered after the fact, when the business strategy has already been

Figure 1—Interrelationship of Val IT Framework 2.0 and Processes



Value Governance (VG)

Establish informed and committed leadership.

Define and implement processes.

Define portfolio characteristics.

Align and integrate value management with enterprise financial planning.

Establish effective governance monitoring.

Continuously improve value management practices.

Portfolio Management (PM)

Establish strategic direction and target investment mix.

Determine the availability and sources of funds.

Manage the availability of human resources.

Evaluate and select programmes to fund.

Monitor and report on investment portfolio performance.

Optimise investment portfolio performance.

Investment Management (IM)

Develop and evaluate the initial programme business case.

Understand the candidate programme and implementation options.

Develop the programme plan.

Develop full life cycle costs and benefits.

Develop the detailed candidate programme business case.

Launch and manage the programme.

Update operational IT portfolios.

Update the business case.

Monitor and report on the programme.

Retire the programme.

Source: IT Governance Institute, *Enterprise Value: Governance of IT Investments*, *The Val IT Framework 2.0*, 2008

determined. Technology today opens up new opportunities that should be considered when business strategy is developed.

- Alignment of value management practices with enterprise financial planning practices. Decisions are too often constrained by the annual budget cycle, outdated bookkeeping practices and the inflexible processes surrounding them.
- Linkage of the expected benefits of investments to business targets, forecasts and budgets to reinforce accountability and facilitate monitoring
- The availability of IT and business human resources needed to deliver the technology capabilities and implement the business changes required to realize value from those capabilities
- Distinguishing between measuring the performance of solution delivery, providing capabilities and service delivery, operationalizing capabilities and benefits realization, and using the capabilities to create business value

Deepening the Framework

Management guidelines for each Val IT process, similar to the COBIT management guidelines, have been added. These include inputs and outputs to illustrate what processes (including COBIT processes) need from others and what the processes typically deliver; activities and associated roles and responsibilities (RACI charts[3]); and goals and metrics.

In addition to the RACI charts for each process, *The Val IT Framework 2.0* also provides a breakdown of accountabilities and responsibilities for Val IT activities by function, e.g., the activities for which the board is accountable and/or responsible. Maturity models—both high-level models and detailed, attribute-level models—are also provided for each of the three Val IT domains, to enable enterprises to assess where they are today and where they want to be.

Guidance on How to Get Started

While Val IT contains essential guidance for any executive interested in establishing a more effective approach to value management, executives are not always clear on exactly how to begin.

What executives and other organizational leaders need is practical advice on how to translate “knowing” into “doing,” i.e., how to close the “knowing-doing” gap.[4] This is especially true because no two enterprises are alike, and understanding how to design, implement and sustain effective value management practices involves enterprise-specific complexities that defy a one-size-fits-all approach. To this end, *The Val IT Framework 2.0* is complemented by a companion publication[5] that provides business and IT executives and organizational leaders with an easy-to-follow guide on getting a value management initiative started. *Enterprise Value: Governance of IT Investments, Getting Started With Value Management* helps the organization by:

- Describing the most common pain points (e.g., limited or no understanding of IT expenditures), signaling a need for better value management, and describing the “trigger events” (e.g., a shift in the market or the economy) that may compel business leaders to begin building such a capability
- Outlining a typical “future state”: what the common characteristics and outcomes of a value-driven enterprise look like

- Providing guidance on how to conduct a high-level assessment of the enterprise's current state
- Explaining how to launch a value management initiative: selecting from one of several proven approaches and identifying the most applicable Val IT processes and practices based on the enterprise's particular pain points and objectives
- Underlining some of the most critical elements in managing the organizational change required to sustain value over time

Future Direction

ITGI is moving toward having a comprehensive, complete, coherent and consistent suite of frameworks and supporting products that will be consistent with an overall architecture and aligned with the needs of different constituencies. To that end, work is currently underway on a risk framework, which will complement and be consistent with Val IT and COBIT. The changes included in *The Val IT Framework 2.0* are intended to move us in this direction. It is anticipated that the next releases of these three frameworks will move us much further.

Conclusion

Even executives who relate to the need for effective governance and management of IT may not recognize that many of the day-to-day business issues they face involve issues of value management. Val IT provides proven value management principles, processes and practices to enable enterprises to maximize the delivery of business value from investments in IT. COBIT complements Val IT by providing the framework for the execution of the IT-related aspects of investments, including IT solution delivery, IT operational implementation and IT service delivery. The risk management framework mentioned earlier will make the picture even more complete. Together, these frameworks will provide the most comprehensive overall guidance to enterprises for the effective governance and management of the delivery and use of IT, and will enable them to maximize value by optimizing benefits at an affordable cost with a known and acceptable level of risk.

The Val IT Framework 2.0 is available in two forms: an extract and a full version. The extract is intended for the reader who wants an overview of Val IT without the detail. The full document is intended for the reader who needs a more detailed understanding of Val IT.

The Val IT Framework 2.0 and *Getting Started With Value Management* can be downloaded at no charge from the ITGI web site, *www.itgi.org/valit*, and can be purchased in hard copy from the ISACA Bookstore, *www.isaca.org/bookstore*.

Endnotes

[1] Thorp, John; "The Drive for Value Management," *Information Systems Control Journal*, vol. 2, 2008

[2] IT Governance Institute, *Enterprise Value: Governance of IT Investments, The Val IT Framework 2.0*, USA, 2008, *www.itgi.org/valit*

[3] A RACI chart identifies who is Responsible, Accountable, Consulted and/or Informed.

[4] Pfeffer, Jeffrey; Robert Sutton; *The Knowing-Doing Gap*, Harvard Business School Press, 2000

[5] IT Governance Institute, *Enterprise Value: Governance of IT Investments, Getting Started With Value Management*, USA, 2008, *www.itgi.org/valit*

John Thorp, CMC, ISP
is president of The Thorp Network Inc. and a consulting fellow with Fujitsu Consulting. He is an internationally sought-after management consultant with 45 years of experience in the information management field. Author of *The Information Paradox*, Thorp's focus is on helping organizations realize the benefits of IT-enabled change. Over the last five years, his work has extended beyond IT to the broader issues of enterprise value management and strategic governance. Working with ITGI, he has been a lead developer of Val IT, and is currently chair of the Val IT Steering Committee and a member of the IT Governance Committee.

Five Questions With...

Tom Gill

As vice president of information technology and chief information officer (CIO), Tom Gill has responsibility for global IT at Plantronics. During his tenure as CIO, Plantronics' revenues have grown from US $200 million to US $850 million, and offices have expanded to 23 countries. Gill leads an IT team that is focused on business outcomes and possesses a passion for partnering and customer service.

Before joining Plantronics, Gill held IT management positions at Bay Networks, Tandem Computers and TRW. He is a member of the Microsoft High Tech Customer Advisory Board; a frequent lecturer in the technology and information management program at the University of California, Santa Cruz; a member of the Cabrillo College CIS/CS Advisory Committee; and a board member on the Santa Cruz County Business Council. In his leisure time, Gill enjoys distance running, playing guitar and cooking.

Question

Having moved from a technical IS/IT background to the position of CIO, how do you believe your background uniquely qualifies you for this role?

Answer

While my focus is on aligning IT and business strategies, my technical background does help in three areas. In cases where we have an outage or other type of incident, I am able to truly grasp the root cause and engage with the team on a technical level. In the area of architecture decisions, I am well equipped to understand not only the business problem to be solved but also the underlying technology. The third area is IT credibility. I can talk feeds and speeds and keep up with the more technical team members, which helps me to be a more effective leader.

Question

How do you see the role of the project management office (PMO) developing over the near term and long term?

Answer

The PMO is key to effective project planning and execution. Over the past two years at my organization, we have implemented a project portfolio management process with an emphasis on aligning IT priorities with strategic business drivers. We have also implemented a project framework based on PRINCE2. The result has been significant improvement in global communication, teamwork and results.

Question

What are the biggest challenges companies are facing in regard to compliance with regulations such as the US Sarbanes-Oxley Act, Basel II and other comparable regulations, now that many of these regulations have been in effect for a few years? What, if any, advantages are companies in compliance reaping?

Answer

At my organization, we welcome the changes because they help us to scale and be a more effective and efficient organization. Plantronics has transformed from a US company doing business globally to a global company. Increasing the maturity of our processes is essential and external drivers help accelerate improvement.

Question

How do you believe the many recent disasters worldwide have changed the way organizations face disaster recovery and business continuity solutions?

Answer

IT is ubiquitous and the impact of a disaster on our ability to operate is significant. At my organization, we are in the process of reviewing our business impact assessment and are finding that the business has less tolerance for downtime than just a few years ago. The bad news is that threats such as natural disasters and pandemics are real. The good news is that technology has advanced in areas such as software as a service (SaaS), replication, teleworking and network design, resulting in more cost-effective business continuity solutions.

Question

In regard to IT risk management, what do you believe is the single largest IT-related risk for businesses today? How do you see organizations meeting or not meeting this challenge?

Answer

It is difficult to identify the single largest risk but, in general, internally hosting Oracle E-Business Suite and Exchange is a risk. IT should be focused on business outcomes vs. technology. At my organization, we are fortunate to have a highly qualified team and a record of high availability. However, the trend of moving to cloud computing and gaining the economies of scale of service providers has a strong business case.

IS Auditing and Information Privacy Governance:

A Natural Fit

By Chris Zoladz, CISA, CIPP, CISSP, CPA

For years information systems (IS) auditors have faced the challenge of convincing business managers of the value they provide to the organization. This was often a daunting challenge. Over time, however, an evolution in general understanding and appreciation of the significant dependence on information systems for virtually every part of the business helped to raise the business's consciousness of the obvious: the security of these information systems is vital to the business, and assurance that these systems are secure is essential.

With the US Sarbanes-Oxley Act requirements, sectoral security mandates (e.g., US Gramm-Leach-Bliley Act, US Health Insurance Portability and Accountability Act), required online privacy disclosures in some states, international data protection laws (e.g., EU Data Protection Directive), myriad US state security breach notification laws and comprehensive credit card company security requirements (the Payment Card Industry [PCI] Data Security Standard [DSS]), the discussion around "why are we even talking about IS auditing?" hopefully is a distant memory. Many business managers now understand "why" it is important and are focusing more on "how" and the financial impact of how the organization addresses these needs. However, the need to continue demonstrating value to the business is a timeless and fair expectation.

This article will focus on an emerging area for which IS auditors are a natural fit for delivering more value to an organization: information privacy governance.

IS auditors are a natural fit for delivering more value to an organization: information privacy governance.

Information privacy is a must for the security mandates mentioned previously as well as an integral element of a number of customer-facing, revenue-generating activities. Specifically, information privacy is an integral element of key business processes surrounding e-commerce, e-mail marketing, telemarketing and doing business in certain international markets. To demonstrate this point, a brief review of e-commerce and e-mail marketing is presented.

E-commerce

For many organizations, conducting business on the Internet is usually the lowest-cost sales channel and thus the one many organizations want to aggressively expand. Secure, privacy-sensitive e-commerce is an absolute requirement to successfully establishing consumer trust, protecting an organization's brand and driving more online business. The privacy officer works with the e-commerce business leaders and information security to ensure that there is an accurate and complete privacy statement posted on the web site, so that customers understand what information is collected, why it is collected, how it will be used, use of cookies or pixel tags, and security measures in place to protect the customer's information. If an organization's web site and associated business practices do not live up to the privacy statement, customer loss and potentially an investigation from, in the US, the Federal Trade Commission and/or a state attorney general's office can be expected. The IS audit function can help assess and manage this risk and add value, protecting a low-cost, revenue-generating sales channel, by conducting a privacy audit of the web site. IS auditors can be a natural fit for this activity as they are experts in auditing information systems and that is precisely what is needed in this case. While this article is not focused on how to conduct a privacy audit of a web site, some of the areas that should be covered are:

- Is a current privacy statement posted?
- Are the disclosures complete and accurate?
- Is the opt-out process functioning as intended?
- Is the P3P version of the privacy statement consistent with the narrative version?

E-mail Marketing

Like selling products or services via a web site, e-mail marketing is often a least-cost channel for promoting products and services. However, e-mail marketing is regulated activity in the US and in some international markets. Also, and as important, poorly executed e-mail marketing can be one of the fastest means to alienate customers. Proper e-mail marketing management includes adherence to the e-mail marketing laws and being aware and sensitive that some consumers will view e-mail marketing messages as an annoyance and intrusion. IS auditors can be invaluable to helping the business protect their e-mail marketing channel from a privacy perspective. Just a couple of the specific areas that could be assessed are:

- Were customers informed that their e-mail address would be used for marketing purposes?
- Has the e-mail marketing list been adjusted for previous opt-outs?
- How are consumer complaints about e-mail messages handled?

Gaining Information Privacy Expertise

While IS auditors can be a natural fit for providing information privacy governance, information privacy is a distinct body of knowledge and training is necessary to be able to competently audit this area. The information privacy profession is relatively new and is being shaped by the International Association of Privacy Professionals (IAPP) just as ISACA did for the IS auditing profession a few decades ago. The IAPP was established to define, promote and improve the privacy profession globally. The IAPP is committed to providing a forum for privacy professionals to share best practices, track trends, advance privacy management issues, standardize the designations for privacy professionals and provide education. The IAPP also sponsors the Certified Information Privacy Professional (CIPP), a certification for privacy professionals.

Conclusion

Progressive value-added IS auditing will continue to evolve over time as technology and business needs evolve. A component of the current-day IS auditing repertoire should include information privacy auditing. This is a natural extension of the skill sets and focus of the current-day IS auditor.

However, this is a new subject matter area that, like any other, requires expanded subject matter expertise. As a long-time Certified Information Systems Auditor™ (CISA®), the author encourages readers to consider expanding their current activities to include information privacy governance and add more value to their enterprise today.

Chris Zoladz, CISA, CIPP, CISSP, CPA
is the vice president, information protection and privacy, at Marriott International Inc. Zoladz is responsible for information protection and privacy strategy, policy development and deployment, security awareness, and compliance strategies to meet information protection/privacy, business and legal requirements. He is a past president and current board member of IAPP and a past board member and treasurer of the National Capital Area (Washington DC, USA) Chapter of ISACA.

Prepare for the **2008** *CISA Exams*

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

Passing the CISA exam can be achieved through an organized plan of study. To assist individuals with the development of a successful study plan, ISACA offers several study aids and review courses to exam candidates (see *www.isaca.org/cisaexam* for more details).

CISA Review Manual 2008

ISACA

The *CISA® Review Manual 2008* has been completely revised and updated with new content to reflect changing industry principles and practices, and is organized according to the current CISA job practice areas. The manual features detailed descriptions of the tasks performed by IS auditors and the knowledge required to plan, manage and perform IS audits. The new edition also features new case studies to assist a candidate's understanding of current practices. Also included are definitions of terms most commonly found on the exam, practice questions similar in content to what has previously appeared on the exam and references to additional study materials on specific topics. This manual can be used as a stand-alone document for individual study or as a guide or reference for study groups and chapters conducting local review courses.

The 2008 edition has been developed and is organized to help prepare the CISA candidate in studying the following job practice areas:

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

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

CISA Review Questions, Answers & Explanations Manual 2008

ISACA

The *CISA® Review Questions, Answers & Explanations Manual 2008* consists of 600 multiple-choice study questions that have previously appeared in the *CISA® Review Questions, Answers & Explanations Manual 2006* and the *2007 Supplement*. Many questions have been revised or completely rewritten to recognize a change in job practice, be more representative of the current CISA exam question format, and/or to provide further clarity or explanation of the suggested correct answer. These questions are not actual exam items, but are intended to provide the CISA candidate with an understanding of the type and structure of questions and content that have previously appeared on the exam. This publication is ideal to use in conjunction with the *CISA Review Manual 2008*.

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

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

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

CISA Review Questions, Answers & Explanations Manual 2008 Supplement

ISACA

Developed each year, the *CISA® Review Questions, Answers & Explanations Manual 2008 Supplement* is recommended for use when preparing for the 2008 CISA exam. This edition consists of 100 new sample questions, answers and explanations based on the current CISA job practice areas, using a similar process for item development as is used to develop actual exam items. The questions are intended to provide the CISA candidate with an understanding of the type and structure of questions that have typically appeared on past exams, and were prepared specifically for use in studying for the CISA exam.

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

CISA Practice Question Database v8

ISACA

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

PLEASE NOTE the following system requirements:

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

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

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

To order CISA review material for the December 2008 exam, see the order form on page S-8 in this *Journal* or visit *www.isaca.org/cisabooks.*

Implementing Information Technology Governance:

Models, Practices and Cases

By Wim Van Grembergen, Ph.D., and Steven De Haes, Ph.D.
Reviewed by Reynaldo J. de la Fuente, CISA, CISM

This is an important book from two professors at the University of Antwerp Management School (UAMS).

The work is divided into five chapters that achieve a good balance of the theoretical and practical aspects of IT governance implementation using *Control Objectives for Information and related Technology* (COBIT®) principles as the main tool.

Chapter one records and interprets some important existing theories, models and practices regarding IT governance and strategic alignment.

Chapter two focuses on how COBIT can be leveraged as an instrument to implement IT governance. All the components of the COBIT framework are explained and guidance is provided on how COBIT can be adapted to or applied in a specific organization.

Chapter three addresses the IT balanced scorecard (BSC) as a measurement and management tool to support the achievement of strategic alignment. The BSC application is illustrated in detail through a case study of a major Canadian financial group.

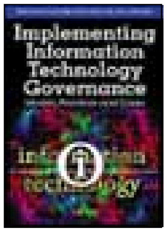
Chapter four describes case studies from different sectors: an insurance company, a bank, a worldwide supplier of chemicals, polymers and packaging, a steel producing company, and an organization of the health insurance sector.

Based on prior research and complemented with practical feedback obtained in the before-mentioned case studies, a set of guidelines and ideas for implementation enhancement is compiled in chapter five.

The work covers almost all of the job practice areas of the Certified in the Governance of Enterprise IT™ (CGEIT™) certification, especially IT governance framework, strategic alignment, value delivery and performance measurement.

The book cleverly emphasizes the distinction between IT management and IT governance:

> *IT management is focused on the effective and efficient internal supply of IT services and products and the management of current IT operations. IT governance in turn is much broader, and concentrates on performing and transforming IT to meet present and future demands of the business (internal focus) and its customers (external focus).*



This effort to raise awareness of the differences between these concepts is extremely important to promote organizational updates, helping in the creation of new IT governance positions.

This work provides an illustration of the possibilities of using COBIT as a recognized practical framework that helps practitioners to establish the most important aspects to back their work. At the same time, it does not tie users down; it gives room for innovation and some personal inclination deployment along the implementation road map.

Reynaldo J. de la Fuente, CISA, CISM
is chief executive officer 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 an 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:

Implementing Information Technology Governance: Models, Practices and Cases 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.

Put down the stress ball. Relax.
Information Governance now has
DLTIYHBTIYN
(Don't Let The Information You Have Bury The Information You Need)

The Handbook of Fraud Deterrence

By Harry Cendrowski, James P. Martin and Louis W. Petro

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

The *Handbook* of *Fraud Deterrence* is written primarily as a guide to assist the fraud deterrence professional. Apart from providing help in setting up fraud deterrence practices in an organization, it also provides valuable insights to management professionals seeking to understand fraud deterrence as a discipline.

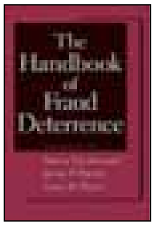
The increase of fraud cases across the world, both in number and magnitude; the growing sophistication of the techniques used by fraudsters; stakeholders' rising expectations of antifraud professionals; and the greater responsibility placed on corporate executives and boards of directors by corporate governance legislations such the US Sarbanes Oxley Act of 2002 have effectively raised the bar and increased the pressure on these professionals. Organizations expect that these professionals will effectively combat fraud and reduce its incidence to an acceptable level. The world of handling frauds has undergone a sea change from being reactive to proactive, from fraud detection to fraud deterrence.

The book is divided into three sections. The first section deals with the professional environment and fraud deterrence and has eight chapters and nine appendices. It provides a general background about fraud deterrence techniques and procedures. The section looks at fraud deterrence as a business management tool, and traces the history of fraud deterrence and the role of professional standards in the development of the discipline. The classic fraud triangle is outlined in chapter five, followed by the human angle to fraud, which explains motivations of employees and the need to promote a disciplined corporate culture, based on judicious use of internal checks and controls.

Section II covers tools of fraud deterrence and has seven chapters. It discusses the tools commonly used to combat fraud including internal control structures, data analysis and monitoring, tools based on information technology, and reporting tools.

Section III has six chapters and seven appendices and covers applications of fraud deterrence, giving a practical perspective to the book. It also provides well-developed examples to enhance its usefulness to the readers.

The book has a number of exhibits, sample formats and reports, flow charts, and numerous references. The chapters follow a logical structure: an introduction and background, followed by development of the topic, a conclusion and notes. *Control Objectives for Information and related Technology* (CobiT) is referred to in the context of the Committee of Sponsoring Organizations of the Treadway Commission (COSO)'s *Internal Control—Integrated Framework* and the business requirements of confidentiality, integrity, availability, effectiveness, efficiency, compliance and reliability of information systems.



The authors have professional expertise and exposure to risk assessment, auditing and expert testimony—all necessary for fraud handling. Furthermore, the many individual contributors, 28 in number, provide their own unique contribution and outlook in terms of subject knowledge and expertise.

The book propagates a proactive perspective to handling fraud that makes good business sense.

Given the seriousness of fraud and the adverse impact it has on business objectives, it is a good idea to prevent fraud. This is even more important in small and medium-sized businesses, which are often hardest hit by fraud. But, it also holds true for the corporate, public companies that are accountable to a wide spectrum of stakeholders.

In fact, it would, in the end, not be wrong to conclude that fraud deterrence is an effective management tool that ensures less leakage of revenues, greater efficiency of the business and, ultimately, a better bottom line.

The book has a useful glossary that defines and explains fraud-related terms and abbreviations. It is followed by an index that is fairly comprehensive and provides cross-referencing.

In conclusion, the book brings out the intricacies in dealing with fraud in a professional manner and reflects the efforts put in by the authors and contributors to give the book a practical orientation.

Vishnu Kanhere, Ph.D., CISA, CISM, AICWA, CFE, FCA is an expert in software valuation, information systems (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; a member of the ISACA Publications Committee; honorary secretary of the Computer Society of India, Mumbai Chapter; convener of the 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:

The Handbook of Fraud Deterrence 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.

Database Security, Compliance and Audit

By Charles Le Grand and Dan Sarel

A major control objective for any organization is to protect sensitive data. Data protection or information security is protecting information and information systems from unauthorized access, use, disclosure, disruption, modification or destruction to provide confidentiality, integrity and availability.[1]

In the early years of database management systems (DBMS), such a system was acclaimed as a tool for centralizing control over data access. But as controls frequently migrate around within the information infrastructure, data access controls have tended to migrate to other points, such as network perimeter controls, user identity and access management, and the application systems that access databases. The tendency has been to presume a database is protected because of the broad and diverse set of controls applicable to data access. However, the breadth and diversity of controls have taken away the centralized access control at the database itself, opened key weaknesses in data protection and allowed some of the most serious threats to data to go largely unmanaged.

There is a strong need for improved and enforced accountability management.

The world is characterized by technology that makes the news almost daily with stories of loss, theft or disclosure of sensitive information. The 2007 Computer Crime and Security Survey, by the Computer Security Institute (*www.gocsi.org*), identifies respondents that actually detected attacks and abuse in the last 12 months. Insider abuse of net access is at 59 percent, unauthorized access to information 25 percent, and theft of customer or employee data 17 percent. (Because of the general lack of monitoring, one can safely assume most threats remain undetected!) These numbers also seem low based on media accounts. And, people are beyond the point of being shocked or even surprised when yet another employee, executive or management team betrays a trust and costs the company and its stakeholders millions or even billions.

Clearly there is a strong need for improved and enforced accountability management, and internal controls are an essential element of accountability assurance. This article will review first the nature of access controls in general and where they are found, and then will discuss access controls at the database level.

Where Are Data Access Controls?

Data access controls tend to be distributed in many organizations. They have evolved to that state by systems groups attacking the problem of the moment, placing controls where they can protect against a given threat, and avoiding performance bottlenecks and impacts on performance caused by using controls such as native logging and protection in the commercial DBMS. Commercial enterprise resource planning (ERP) systems have also contributed to the distribution of controls by seeking to be the all-in-one system solution with minimal reliance on other controls.

The following are some key distributed control types:

- **Perimeter controls** (e.g., firewalls, intrusion protection, malware detection) attempt to keep the bad guys out. But they have two fundamental weaknesses. First, the bad guys are frequently a step ahead of the protection, and once they get in they are hard to find and block. Second, the insider threat is now recognized to be at least as serious as the threat of attack from outside the organization. Perimeter controls have reached a state of maturity where they are recognized as essential, but they are also known to be inadequate against certain attacks and in need of supplementation by other controls.
- **User identity and access management** is the essence of deciding who is allowed to do what and then monitoring to ensure things are as they are supposed to be. However, these controls tend to be dispersed across a wide variety of business functions including policy administration, personnel administration (e.g., keeping up with access privileges as people move to new positions), managing group access rights (e.g., people in payroll can see some human resources [HR] data, but cannot access payroll info), separation of duties (e.g., not allowing the same person to approve new vendors and payments to them), monitoring access rights for application of the least-privilege principle (e.g., access to only the data needed for the position, limited access for changing or deleting data, special privileges required to override controls), revoking rights when employees or other users leave the company or change roles, and monitoring all changes and exceptions to access privileges rules.

  The subject is complex and requires close coordination across diverse business functions—some of which do not hold information security high on their priorities or the list of things that will get them recognized and promoted. Identity and access management is an area in need of some serious audit attention, but that is the subject of another article.
- **Application systems** (particularly ERP systems) are a focal point for data access protection. And, if user identity and access management is complex, application systems can be more so. Applications administer remote (sometimes global) access by customers, remote and local employees, and often business partners. Multiple applications may access the same database and be subject to differing sets of controls.

Independent audit software tools[2] are available to audit the management of separation of duties and other controls applicable to the popular ERP systems and other means of addressing user identity and access privileges. Application systems are subject to changes including security patching, maintenance and enhancements by the software provider's and/or system's employees, and emergency fixes to restore operations in the event of outages. Application systems may be maintained and enhanced by the original vendors and/or by outsourced vendors, including offshore providers.

- **Privileged users** have access rights beyond those needed for routine business operations. Database technical and operational controls (such as backup/recovery, system upgrades, checkpoint/restart, maintaining pointer integrity, optimizing physical data storage and performance) take place outside of the access constraints of application systems and most of the identity and access management processes, but must also be closely coordinated with application and user requirements. They are perhaps the most important point for knowing exactly who did what with the data.

  Systems and network administration, data and database administration, security operations, systems development and maintenance, systems programming, and other technical functions (sometimes called "superusers") are a security management topic in their own right. All have legitimate needs for access to databases to perform maintenance, test changes, correct problems, and restore or continue operations. Some believe the people in these functions cannot be controlled or monitored. While that is not true, such control may be difficult and one can count on those people to resist control changes they may see as making their jobs more difficult or impossible.

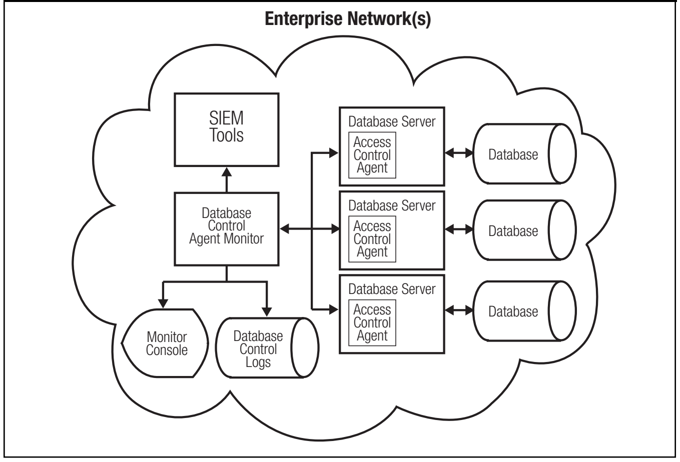
  It is important to note that the technical people with access to databases for the most part reliably perform a crucial function, and the enterprise's systems and services could not operate without their ongoing support. However, as recent breaches have clearly shown,[3] they also represent significant risk as they could easily corrupt, destroy or steal copies of sensitive data, and must be subject to separation-of-duties controls and monitoring, as appropriate to their elevated level of authority and trust. Physical and logical controls within and outside their sphere of operational control are needed to provide evidence of their actions, and must be sufficient to clearly establish fault or innocence.

Centralized Data Access Controls

A time-proven rule for protection and monitoring is to provide controls as close as possible to the functions subject to the controls. In the case of database access controls, the ideal location is on the database server. Not only does this simplify the access protection model, it supports separation of duties, forensics and audit requirements, and can make it difficult for anyone to avoid or bypass those controls.

The controls can also be provided via a network security appliance.[4] But those controls are apart from the device that actually manages the database and, therefore, can be bypassed by people with physical or superuser access to the server. They are also less effective than host-based solutions in monitoring privileged users (such as database administrators and application developers). This discussion addresses the controls as implemented via the agent and monitoring system depicted in **figure 1**.

Figure 1—Database Access Protection Example Diagram



This simple solution employs a software agent that runs on the database server, enabling policy-based data access protection and monitoring.[5] By communicating with a separate system (i.e., the database control agent monitor), the agent can ensure that it has not been modified by persons with administrative access to the database. Note, the agent should be capable of operating in a monitoring-only mode for analysis, discovery or audit purposes, or in a full-protect mode to enforce security policy at the database level.

This type of centralized database access control provides a focal point for knowing exactly who accessed what data—not just that access was granted to a trusted application, in which case one would have to turn to the application for such evidence. It is also not subject to the limitations of identity access management or applications, because the policy can be specified right in the agent itself. And, if protection (preventive controls) is enabled, rather than just monitored (detective controls including alerts for inappropriate access attempts), the agent can be tuned to specifically manage known threats to data.

Protection From Software Vulnerabilities

Software vulnerabilities subject to exploit can occur in many places throughout systems and networks: web pages and other Internet-facing systems; systems that communicate across the Internet, such as through e-mail and file transfer; and even DBMS. Vendors frequently provide patches for software vulnerabilities, but change management (particularly patch management) is fraught with its own challenges and changes, and patches may not be applied in a timely manner (if at all). This leaves the vulnerabilities to be managed by "some other means."[6]

While many exploit attempts today still seek to satisfy the attacker's ego or perhaps embarrass the target enterprise, the real threats are in stealing or manipulating data for profit whether by insiders, outside attackers or perhaps insiders cooperating with outsiders (including organized crime). Inasmuch as the database is a prime target for attacks, it makes sense to place controls around the database to enforce access policies and protect the data, even if other protective controls are compromised. The concepts of compensating, complementary and redundant controls recognize that individual controls are fallible and secondary controls are needed to detect when primary controls fail.

An effective access protection control will recognize inappropriate data access attempts, because they violate an information security policy, even if they appear to come from a trusted application system or a trusted individual with the ability to bypass other system and network controls. Of course, not every exception can be determined in advance, so it may be necessary to apply monitoring controls to certain privileged users, such as the database administrator (DBA), rather than taking a chance on preventing them from performing necessary tasks. But, it is still essential to log and monitor every procedure performed against a database, especially when the procedure affects sensitive data.

Hardening of databases is not a one-time procedure.

While they are not yet common, it is possible to implement controls specifically to compensate for known system vulnerabilities and their related exploits.[7]

Other solutions include custom designed procedures and programs specifically to monitor or protect against (or mitigate) known vulnerabilities that cannot feasibly be eliminated. An example of this type of control is one of a broader nature, focused on specific vulnerabilities in change management. This solution establishes a signature for sensitive components within a network configuration and terminates any task that attempts at processing and would change the signature.[8] In this example solution, the software provider must be constantly vigilant to ensure that new and emerging threats are addressed in the protection.

Hardening System Components to Enhance Database and Access Controls

Applications, network devices and even personal computers can be "hardened" to enhance their protection against known types of attacks. Hardening is the process of securing a system especially to protect it against attackers. It is one of the most efficient ways to combat vulnerabilities.

Hardening typically includes removal of unnecessary usernames or logins and disabling or removing unnecessary services. By removing all system components that are never used, an enterprise can remove all the known, and as-yet-unknown, vulnerabilities that these components bring with them.

Database security may require hardening of the security settings of the database management software upon installation and once a specific database (often referred to as an instance) is established and configured. Additionally, many database utilities have their own enhanced security that can be enabled, but is disabled by default. An example is establishing the password on the Oracle listener process, to ensure that unauthorized users cannot change configurations related to the database management software.

The Center for Internet Security (CIS)[9] provides how-to guidance and tools to harden systems. CIS benchmarks support available high-level standards that deal with the why, who, when and where aspects of IT security by detailing how to secure an ever-widening array of workstations, servers, network devices and software applications in terms of technology-specific controls. CIS scoring tools analyze and report system compliance with the technical control settings in the benchmarks.

Hardening of databases is not a one-time procedure. Any new database must be hardened, and hardening must be undertaken with every upgrade of the DBMS as well as the operating system that runs it. New threats can also bring about changes in hardening processes. Resources such as those from CIS must be constantly monitored for new hardening guidelines, as they change frequently.

Database Access Protection and Compliance Requirements

Information security requirements must provide a proper balance between too much access control and too much freedom of access. Compliance requirements vary by industry and type of company, and each enterprise must interpret the requirements and manage its activities accordingly. There is no silver bullet to ensure compliance. Compliance is best accomplished by meeting requirements and ensuring that the ways in which requirements are met actually provide effective security and accountability.

Compliance alone is merely meeting a baseline set of minimum requirements, and the minimum is rarely sufficient. An organization can be in compliance with many requirements, but still not have effective security. The goal is to provide security first, and compliance as required.

The Payment Card Industry (PCI) Data Security Standard (DSS) is a good example of information security requirements with broad applicability. PCI requirements have gained stature in recent years and they apply to any enterprise that processes, stores and transmits cardholder account data. PCI compliance must be demonstrated and documented through automated and manual system audits.

The 12 major PCI DSS requirements (see **figure 2**) are structured to promote effective information security policies, secure networks, protected cardholder data, vulnerability management, strong access controls, and regular monitoring and testing. Central to all PCI requirements is the need to protect data access to ensure accountability, privacy and data integrity. The simple goal is to ensure that only authorized individuals have access and all access is monitored. To limit access to only people whose jobs require it, access protection must apply to identifying the sensitive data elements; the methods for managing user credentials and access rights; and the records of who accessed what, when and what they did with it.

Figure 2—PCI DSS Requirements in a Nutshell

Build and Maintain a Secure Network
1. Install and maintain a firewall configuration to protect cardholder data.
2. Do not use vendor-supplied defaults for system passwords and other security parameters.

Protect Cardholder Data
3. Protect stored cardholder data.
4. Encrypt transmission of cardholder data across open, public networks.

Maintain a Vulnerability Management Program
5. Use and regularly update antivirus software.
6. Develop and maintain secure systems and applications.

Implement Strong Access Control Measures
7. Restrict access to cardholder data by business need-to-know.
8. Assign a unique ID to each person with computer access.
9. Restrict physical access to cardholder data.

Regularly Monitor and Test Networks
10. Track and monitor all access to network resources and cardholder data.
11. Regularly test security systems and processes.

Maintain an Information Security Policy
12. Maintain a policy that addresses information security.

(Source: *https://www.pcisecuritystandards.org/pdfs/pci_dss_v1-1.pdf*)

A particular enterprise's compliance requirements may not include those of PCI DSS. If that is the case, they can accumulate their own list of compliance requirements from policies, procedures, agreements with customers and business partners, industry guidelines and requirements, regulations, and legislation. But PCI DSS is innovative, strong and quite clear guidance (as opposed to many other standards), and is applicable to any sensitive data in a database.

However, regardless of the solution, one should find information access protection at the heart of the requirements.

Database Access Control Objectives

A key component for identifying the steps in a database access protection audit is to identify the risks associated with the data maintained in the database and the potential impacts if risks materialize. For each control objective, the auditor must assess the specific controls in place and consider the risks and consequences if the objectives are not consistently and continuously met. Database access control objectives include:

- Appropriate assignment of responsibilities including separation of duties
- Access allowed only as appropriate (no unauthorized access)
- Completeness and accuracy of data in the database
- Evidence that each transaction or update is accurately applied and recorded
- Appropriate management of data sharing
- Adequate transaction/access audit trails
- Adequate service level for database users
- Data recorded in the appropriate calendar period
- Ability to detect and recover any failure of the DBMS
- Sufficient evidence and analysis to detect and recover from attack, fraud or embezzlement
- Current and adequate documentation. Documentation to include for database structure:
  – How security is achieved
  – Recovery actions
  – Reorganization changes

  Documentation to include for each data element:
  – Precise and unambiguous definition
  – Source
  – Frequency of change
  – Individual accountable for correctness
  – Relationship to other data items
  – Program(s) and individuals with authorized access and the type of access
  – Physical devices authorized to access (e.g., payroll department only)
- Continuity of processing
- Compliance with internal and external policies, standards and requirements
- Effective management of systems development, maintenance and changes/patches
- Periodic independent database audits

This list of control objectives was selected for relevance to database security and access control. A broader scope audit program is required for audits with a different purpose or objective.

Auditing Database Access

Conceptually, database auditing focuses on answering some fairly basic questions: How does one know, and how can one verify who accessed and/or changed the data? When? How was the content changed? The difficult part lies in assessing the full scope of controls to determine their effectiveness in fully recording all accesses; ensuring only authorized access; and maintaining unimpeachable evidence for management, audit, assurance and forensics purposes.

Database controls and audits must address:

- User interfaces
- Operation of the DBMS
- Database administration
- Data definition and documentation
- Security and access
- Organizational policies and priorities
- Backup and recovery
- Business continuity
- Compliance with standards and requirements

However, not all of these areas are necessarily relevant to an audit of database access management and compliance. Each area of database management has its own set of control objectives, and the objectives frequently apply to multiple areas.

Auditors must audit, evaluate and test the controls they find in place for database protection and monitoring, and their assessment must be of the existing controls rather than the controls they believe should be in place. However, audit recommendations can focus on moving the enterprise to a more reliable and efficient approach to information protection and access control.

Conclusion

To summarize, access protection begins with understanding who accesses the data, for what purposes and with what permission. The set of controls relevant to database access management is broad and complex, and touches many areas of the business and technology.

The way to solve a set of problems as large and complex as information access protection is to establish priorities and begin solving the most significant problems first, one at a time, within an overall plan to provide and maintain a reasonable level of risk and substantial compliance with requirements.

At the core of business controls over information is the need to protect data access to ensure accountability, privacy and data integrity. The simple goal is to ensure only authorized individuals have access and all access is monitored. To limit access to only people whose jobs require it, access protection must apply to identifying the sensitive data elements; the methods for managing user credentials and access rights; and the records of who accessed what, when and what they did with it.

A single source for recording all access to the database is an efficient approach to controls, assurance and auditing, and can be significantly less demanding than the effort needed to manage or audit controls based in multiple locations. When controls are centralized in a single source, they facilitate the ability to verify compatibility across multiple operational areas. One may hear that the DBMS controls cannot be activated because they impact performance too severely. And, while that may be true, the alternative controls described above can provide a reliable centralized access control and can do it efficiently without negatively impacting system performance.

Author's Note

This article is based on a larger work authored by Charles Le Grand and Dan Sarel, published in the April 2008 issue of *EDPACS*, available at *www.informaworld.com/smpp/content~content=a792908951~db=all~order=page*.

Endnotes

[1] Cornell University Law School, US Code Collection, Title 44 US Code § 3542 (b)(1) (2006) as currently published by the US government. This reflects the relevant laws passed by US Congress as of 2 January 2006.

[2] Examples of providers of such tools include Approva, *www.approva.com*; Aveksa, *www.aveksa.com*; and Security Compliance Corp., *www.securitycompliancecorp.com*.

[3] See, for example, the case of Fidelity National Information Services where a database administrator stole 8.5 million customer records and sold the information to data brokers.

[4] Examples include Guardium, *www.guardium.com*; Imperva, *www.imperva.com*; or Tizor's Mantra, *www.tizor.com*.

[5] The only example of such a solution that the authors are aware of is Hedgehog by Sentrigo, *www.sentrigo.com*.

[6] A treatise on change and patch management, with clues as to why patches may not be applied, can be found in The Institute of Internal Auditor (IIA)'s *Global Technology Audit Guide*. More technical documents include the IT Process Institute (ITPI)'s *Visible Ops Security,* the update to the *Visible Ops Handbook* (*www.itpi.org*).

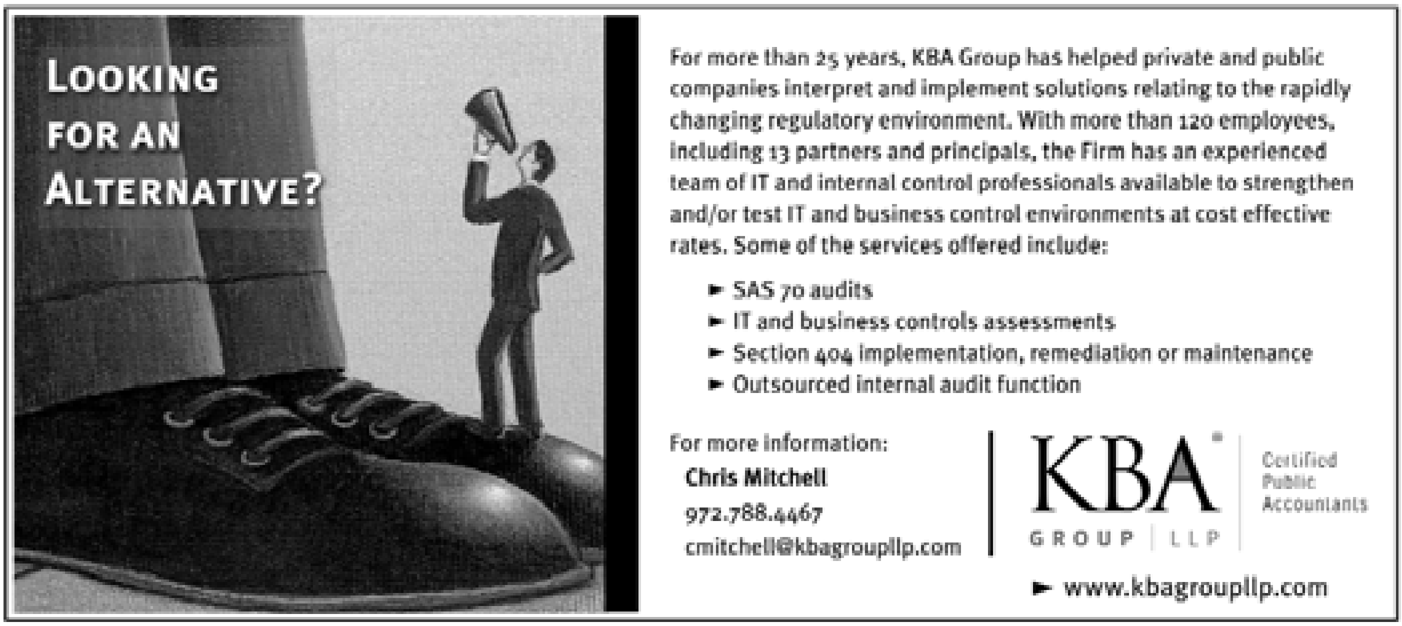
[7] The authors are only aware of one solution for database protection that provides vulnerability protection at the database server for known vulnerabilities in DBMS software: Sentrigo.

[8] Tripwire (*www.tripwire.com*) and Network Authority, by AlterPoint (*www.alterpoint.com*) are examples of this type of control that protects against unauthorized changes.

[9] Center for Internet Security, *www.cisecurity.org*

Charles Le Grand
is a principal advisor of the TechPar Group, and the former director of research and technology for The IIA Inc.

Dan Sarel
is the vice president of Sentrigo Inc. and is responsible for directing Sentrigo's product definition and design.



Prepare for the **2008** *CISM Exams*

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

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

CISM Review Manual 2008

ISACA

The *CISM® Review Manual 2008* has been completely revised and updated with new content to improve consistency and clarity and to remain current in a dynamic field. The updated manual reflects the fact that the information security management profession is rapidly evolving, with increasing responsibilities, scope and authority. Topics covered include governance and management, strategy and policy, security architecture and metrics, and the alignment of security activities with, and in support of, overall business objectives. The new edition also features definitions of terms most commonly found on the exam, practice questions similar in content to what has previously appeared on the exam and references to additional study materials on specific topics. The *CISM Review Manual 2008* is designed to assist candidates in preparing for the CISM exam, and for individuals wanting to learn more about the roles and responsibilities of an information security manager. The manual can be used as a stand-alone document for individual study or as a guide or reference for study groups and chapters conducting local review courses.

The 2008 edition is organized to help prepare the CISM candidate in studying the following job practice areas:

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

CM-8	English Edition
CM-8J	Japanese Edition
CM-8S	Spanish Edition

CISM Review Questions, Answers & Explanations Manual 2008

ISACA

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

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

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

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

CISM Review Questions, Answers & Explanations Manual 2008 Supplement

ISACA

Developed each year, the *CISM® Review Questions, Answers & Explanations Manual 2008 Supplement* is recommended for use when preparing for the 2008 CISM exam. Each edition consists of 100 new sample questions, answers and explanations based on the current CISM job practice areas, using a similar process for item development as is used to develop actual exam items. The questions are intended to provide the CISM candidate with an understanding of the type and structure of questions that have typically appeared on past exams, and were prepared specifically for use in studying for the CISM exam.

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

CISM Practice Question Database v8

ISACA

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

PLEASE NOTE the following system requirements:

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

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

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

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

J-SOX Challenge:

Efforts to Comply With the New Japanese Regulation

By Kazuhiro Uehara, CISA, CIA, PMP, Megumi Yamase, CISA, System Auditor (METI), Shun Miura, CISA, CIA, CCSA, Waka Tsumakawa, CISA, Kenjiro Funaki, CISA, CPA, Koji Takaura, CISA, System Auditor (METI), and Akihiko Ito, CISA, System Auditor (METI)

In 2004, after discovering untrue entries in the financial statements in a railway company, the Financial Services Agency of Japan (FSA) investigated some public companies and also found untrue entries in their financial statements. As a result, the Business Accounting Council for the FSA began deliberations on the effectiveness of management review on financial reporting and on audit practices by public accountants.

The Financial Institution and Exchange Laws, passed by Diet in June 2006, is now known as the Japanese version of the US Sarbanes-Oxley Act or "J-SOX." J-SOX requires the same internal controls over financial reporting as the US Act. The requirements of J-SOX include disclosure of accounting entries as well as financial reporting and its annotation. See **figure 1** for a breakdown of the two regulations.

In light of this new regulation, applicable to all Japanese public companies since 1 April 2008, the Business Accounting Council issued a report, "On the Setting of the Standards and Practice Standards for Management Assessment and Audit Concerning Internal Control Over Financial Reporting (Council Opinions): Practice Standards" (Practice Standards) and established a new internal control framework that is similar to the Committee of Sponsoring Organizations of the Treadway Commission (COSO) report.

Practice Standards

Practice Standards is composed of three sections:

- Basic Framework of Internal Control
- Assessment and Report on Internal Control Over Financial Reporting
- Audit on Internal Control Over Financial Reporting

Basic Framework of Internal Control shows the definition and conceptual framework of internal control. Assessment and Report on Internal Control Over Financial Reporting and Audit on Internal Control Over Financial Reporting indicate the framework of assessment standards by management and the audit by public accountants.

Framework of Japanese Internal Control

In principle, an internal control is a process to achieve the four enterprise objectives:

1. Effectiveness and efficiency of business operations
2. Reliability of financial reporting
3. Compliance with applicable laws and regulations relevant to business activities
4. Safeguarding of assets

The process consists of six basic components:

1. Control environment
2. Risk assessment and response
3. Control activities
4. Information and communication
5. Monitoring
6. Response to IT

One difference between Practice Standards and the COSO framework is that Practice Standards indicate "safeguarding of assets" as an objective distinct from the three others and it adds "response to IT" to the basic five components in consideration of the current reality of IT's deep penetration into enterprises.

Growing Awareness of the IT Frameworks

In accordance with information systems (IS) audit awareness in Europe and the US since the 1980s, Japanese IS specialists have seen the need for their own IS audit practices. While Japanese IS audit and security frameworks were developed and disseminated to the specialists, the international frameworks, such as *Control Objectives for Information and related Technology* (CobiT®), have also been recognized gradually.

There is no official framework for J-SOX IT control issues beyond what is included in Practice Standards, and Japanese enterprises are expected to choose and use the existing IT frameworks according to their conditions. Major Japanese IT frameworks are described in the following sections.

System Management Standards

The System Audit Standards were established in 1985 by the Ministry of International Trade and Industry (MITI), which was reorganized in 2001 into the Ministry of Economy, Trade and Industry (METI), and have been widely used among public/private organizations. In 2004, the standards were divided into two frameworks—the System Audit Standards (SAS), as a code of conduct for the auditors, and the System Management Standards (SMS), as practical standards or a measuring stick to be used for IS auditing. In 1985, MITI introduced the System Auditor qualification and enhanced its human resources development programs in line with the System Audit/Management Standards.

According to the Japan Information Technology Engineers Examination Center (JITEC), which administers the System Auditor examination, the examination assesses an examinee's ability to "deal with safety, efficiency, reliability, availability, confidentiality, maintainability, usefulness, strategic benefits and other factors from a position independent of the

Figure 1—Breakdown of US Sarbanes-Oxley Act and J-SOX[2]

	US Sarbanes-Oxley Act	J-SOX
Governing laws	• Sarbanes-Oxley Act of 2002 (Signed by President, July 2002)	• Financial Institution and Exchange Laws (Passed by Diet, June 2006)
Organizations subjected to rules	• All public companies listed on a US stock exchange	• All public companies listed on a stock exchange in Japan and other companies requested by ministerial ordinance
Type of controls subjected to the rules	• Disclosure controls and procedures (Section 302) • Internal control over financial reporting (Section 404)	• Disclosure controls and procedures (Section 24-4-22) • Internal control over financial reporting (Section 24-4-4)
Type of information subjected to the rules	• Significant disclosures in quarterly and annual reports (Section 302) • Financial statement and footnotes included in 10K, 10KSB,10Q,10QSB, 20F, 40F (Section 404)	• Disclosures included in the Securities Report (Section 24-4-22) • (Consolidated) financial statements and their footnotes in the financial section of the Securities Report (Section 24-4-4) • Disclosures that have a significant impact on the reliability of financial statements in other sections of the Securities Report
Evaluation of IT controls	• Relevant application and general IT controls based upon risk-based approach	• The following controls should be evaluated: 1. IT general controls 2. IT application controls
IT general controls	Consider: 1. Program development 2. Program change 3. Computer operations 4. Access to programs and data	Consider: 1. Management of development and maintenance of system 2. System operation and management 3. System security management, such as access controls 4. Contract management related to service organizations
Definition of deficiencies	1. Deficiency 2. Significant deficiency 3. Material weakness	• Two types based on quantitative and qualitative factors: 1. Deficiency 2. Material deficiency • Five percent of consolidated pretax income is provided as an example of a materiality threshold; however, consideration should be given to the materiality for the financial statement audit.
Subject of audit	• Audit of internal control over financial reporting	• Audit of the effectiveness of management's assessment of internal control over financial reporting

departments being audited and from the viewpoint of management to assess whether the information systems are contributing to corporate management, can evaluate systems based on criteria formed by envisioning ideal systems and can provide constructive guidance for solving problems."[1]

In March 2007, the *System Management Standards Supplement* (SMS supplement) was published to address J-SOX issues. Although J-SOX requires Japanese enterprises to comply with Practice Standards, issued by the FSA, and the SMS supplement is just one of the reference materials, the supplement is commonly referred to by many enterprises that have adopted SMS.

Information System Audit Guidelines for Banking and Related Financial Institutions

The FSA issued a financial inspection manual to regularly supervise institutions such as banking, securities and insurance companies. In 1987, the Center for Financial Industry Information Systems (FISC) established the "Information System Audit Guidelines" for financial institutions to enhance reliability of the information systems on which their business functions heavily depend. In March 2007, the third edition of the guidelines was issued to comply with J-SOX and other revised new acts, and to reflect social trends. The aim of this third edition is not only to comply with J-SOX, but to address all the other issues surrounding information systems. IS departments of financial institutions have made use of the guidelines as their primary J-SOX reference material.

Among other frameworks, SMS and COBIT can be seen as comprehensive IT management frameworks holding a central place in complying with J-SOX. The SMS is prevalent in Japan and will continue to be used among enterprises, although it does not fully take in a management view of IT governance. On the other hand, COBIT has become more attractive to the global business as a workable alternative. Now, the Japanese business addresses the IT control issues by using these two main frameworks, as well as other frameworks.

Approach to J-SOX

The following describes approaches to J-SOX for auditing firms and public companies.

Auditing Firm

In addressing J-SOX, a gap is seen between the roles of auditing firms and the expectation of client companies. Due to two main limitations—audit independency and human resources—it is hard for firms to assume a leadership role to the extent most clients expect:

1. **The client's expanded requirements**. Immediately after J-SOX was enacted in 2006, the client companies of auditing firms began requesting that they address J-SOX issues.

2. **The scarcity of human resources for these specific services**. Compared with 330,000 public accountants in the US, Japan has merely 23,000 Certified Public Accountants (CPAs). Also, the firms have to mitigate their own business risks to comply with social trends and the financial agency's strict inspection. Firms have tried to acquire more audit staff, but the experienced staff, especially those with Sarbanes-Oxley experience, is hard to find in Japan.

   Furthermore, the timing of this law's application has coincided with the revolution of the Japanese audit business; therefore, it has been tough for most of the firms to address J-SOX issues.

Public Company

About 4,000 pubic companies are listed under coverage of J-SOX. As for J-SOX compliance, there is no exception with regard to company size, audit scope and time, to be applied to listed companies. Since most Japanese companies set their fiscal year starting in April, they were to be in compliance with J-SOX by April 2008.

Three types of companies prepared for compliance:

1. **US Sarbanes-Oxley-experienced company**—Approximately 40 Japanese companies have been listed on the US stock exchange markets and have already complied with the US Act. They only have to disclose additional accounting information required by J-SOX, and no other actions should be needed. The holding company of a Japanese bank listed on a US market has already finished US Sarbanes-Oxley-required documentation and control testing, thus additional work would not be needed for J-SOX (at least, that is the expectation).

   When considering "beyond (or after) J-SOX," some of those listed companies utilize global frameworks such as COBIT to establish IT governance, including effectiveness and efficiency of business management beyond the narrow scope of internal control over (just) financial reporting. They institute COBIT-based guidelines, rules and audit programs. Most of these efforts are made by their internal functions, such as the IT strategy design or the internal auditing sections.
2. **Non-Sarbanes-Oxley-experienced company**—For many Japanese companies, complying with an internal control regulation such as J-SOX is their first such compliance effort, and they are preparing for it with the help of advisory or consulting services. However, due to the lack of Sarbanes-Oxley specialists in the region, the service charges are extremely high. In the case of IT control services, the skill and knowledge of IT general controls and application controls are different. This means companies have to pay for each service respectively. For small and medium-sized companies that do not have enough money to pay for the services, even the documentation charges are so expensive that they have to rely on Sarbanes-Oxley templates or related guidebooks to address J-SOX on their own.
3. **Affiliate company**—If an affiliate company is not listed on the stock market, but its corporate is, it might be regarded as a strategically important subsidiary and have to address J-SOX. In 2006, such companies focused on their business-critical processes, selected risks on them, documented related controls and assessed the design status of the controls.

   They could choose one of two audit policies with which to move forward:
   - Focus on the processes affecting accounting impact on its corporate financial statement.
   - As a single company, focus on the processes affecting its own financial statement.

Affiliate companies chose the latter option because they viewed the compliance challenge as a chance to increase their internal controls. The first step was to send requests for proposals (RFPs) to service providers such as consulting, auditing and IT vendor companies. These companies found it difficult to find firms even willing to complete the RFP process, and frequently found that they had no choice but to contract with the vendor that had provided services for their previous year's trial project. Next, the project team was established. With the chief financial officer (CFO)'s assistance and the business planning and general affairs departments as project leaders, the core members of the accounting, operation and IT department staff set the project management office and made a two-month core plan. The business operation audit department assumed the assessment role of the design/operational status of the controls. From the early stages of the planning phase, the team shared information about critical decision matters such as audit policies, accounting entries, operation processes and IT (platform, application and network) with their auditing firm and asked for the firm's advice on such matters.

Market Trend Around J-SOX

Listing companies are rushing to establish the essentials of an internal control system that meets J-SOX requirements. In Japan, the IT industry has taken the lead in expanding the J-SOX compliance markets.

Consulting Services

J-SOX consulting services are provided most commonly by the Big 4 auditing firms and their group consulting firms. However, these audit firms face a lack of resources for such consulting services. Additionally, the IT industry in Japan has been on track for a revival, making it more difficult to get appropriate consulting services for J-SOX projects.

IT Tools

There are several types of IT solutions to support J-SOX compliance, which provide:

- Support documentation and evaluation
- Improved application controls
- Improved general IT managemen
- Improved company-level controls

Human Resources

Listed companies are willing to hire more staff: internal auditors and Sarbanes-Oxley-experienced system auditors. As mentioned earlier, there is not enough skilled staff who can handle the J-SOX compliance issues.

From the perspective of J-SOX-related qualification, staff requirements include:

- Japan Certified Public Accountant (JICPA)
- Certified Public Accountant (CPA) from the American Institute of Certified Public Accountants (AICPA)
- Certified Internal Auditor (CIA) from the Institute of Internal Auditors (IIA)
- Certified Information Systems Auditor (CISA) from ISACA
- System Auditor from METI

Conclusion

Since the J-SOX Act was passed by Diet in June 2006, Japanese public companies have made enormous efforts to comply with the Act by referring to Practice Standards and IT frameworks such as SMS.

There are many participants in this compliance race. Auditing firms, US Sarbanes-Oxley-experienced/nonexperienced companies and US affiliate companies are trying to address this challenge in their own way.

However, Japan still needs more human resources for J-SOX and related IT control specialties. To overcome this challenge, Japan should increase knowledge and skills of the business and IT internal controls, and set out for a new governance scheme beyond Sarbanes-Oxley.

References

US Congress, Sarbanes-Oxley Act of 2002, USA

Financial Services Agency of Japan Business Accounting Council, "On the Setting of the Standards and Practice Standards for Management Assessment and Audit Concerning Internal Control Over Financial Reporting (Council Opinions)," 15 February 2007

IT Governance Institute (ITGI), COBIT 4.0, Japanese version, 2005

IT Governance Institute (ITGI), COBIT 4.1, 2007

IT Governance Institute (ITGI), *Enterprise Value: Governance of IT Investments, The Val IT Framework*, 2006

IT Governance Institute (ITGI), *IT Control Objectives for Sarbanes-Oxley, 2nd Edition*, Japanese version, 2006

Committee of Sponsoring Organizations of the Treadway Commission (COSO), *Internal Control—Integrated Framework*, USA, 1985-2006

Committee of Sponsoring Organizations of the Treadway Commission (COSO), *Enterprise Risk Management—Integrated Framewor*k, USA, 2004

Ministry of Economy, Trade and Industry (METI), System Management Standards, Japan, 2004

Ministry of Economy, Trade and Industry (METI), System Audit Standards, 2004

Ministry of Economy, Trade and Industry (METI), *System Management Standards Supplement*, 2007

The Center for Financial Industry Information Systems (FISC), "Information Systems Audit Guidelines for Banking and Related Financial Institutions," Japan, 1987

Endnotes

[1] Information-technology Promotion Agency, Japan (IPA) and Japan Information Technology Engineers Examination Center (JITEC), "Examination Categories and Typical Examinees," *www.ipa.go.jp/about/english/index.html*, 2007

[2] Protiviti Japan Co. Ltd., "Japanese Guidelines for Internal Control Reporting Finalized—Differences in Requirements Between the US Sarbanes-Oxley Act and J-SOX," *J-SOX Flash Report*, 2007

Kazuhiro Uehara, CISA, CIA, PMP
is a consulting manager specializing in IT management and IT governance at the Hitachi Consulting Co. Ltd. Uehara is a member of the ISACA Tokyo Chapter's Research Board and one of the coleaders of the *Information Systems Control Journal* reading session. Uehara also contributes to translation review for the ISACA Tokyo Chapter and ITGI Japan.

Megumi Yamase, CISA, System Auditor (METI)
is a core team member of the *Information Systems Control Journal* reading session and contributes to translation review for the ISACA Tokyo Chapter and ITGI Japan.

Shun Miura, CISA, CIA, CCSA
is a core team member of the *Information Systems Control Journal* reading session.

Waka Tsumakawa, CISA
is one of the coleaders of the *Information Systems Control Journal* reading session and contributes to translation review for the ISACA Tokyo Chapter and ITGI Japan.

Kenjiro Funaki, CISA, CPA
is a past leader and a core team member of the *Information Systems Control Journal* reading session.

Koji Takaura, CISA, System Auditor (METI)
is a technical director specializing in IT management and IT governance at the Hitachi Consulting Co. Ltd. Takaura is the ISACA Tokyo Chapter Research Board standing director and a core team member of the *Information Systems Control Journal* reading session. Takaura also contributes to translation review for the ISACA Tokyo Chapter and ITGI Japan.

Akihiko Ito, CISA, System Auditor (METI)
is a core team member of the *Information Systems Control Journal* reading session and contributes to translation review for the ISACA Tokyo Chapter and ITGI Japan.

Control Issues of Using Corporate Web Sites for Public Disclosure

By Antonio Wong, Ph.D., CFA, and Pak-Lok Poon, Ph.D., CISA, CSQA, MACM, MIEEE

Regulation Fair Disclosure (Reg FD), which took effect in 2000, has changed the rules of the game regarding how information is disseminated. Basically, Reg FD requires that when a listed firm in the US disseminates "material" information, it does so publicly.[1] Examples of material information include major corporate events (e.g., mergers and acquisitions), internal operational statistics, earnings forecasts and advance warnings of earning results. Without doubt, this information is essential for the investors to make sound investment decisions. As such, Reg FD is an initiative specifically introduced by the US Securities and Exchange Commission (SEC) to prevent selective disclosure or actions that might benefit one investor over another.

The main purpose of this article is to discuss in detail the related control issues that arise when a firm attempts to use its corporate web site to fulfill Reg FD. Without the knowledge of such control issues, the attempt is likely to fail. In this regard, the article should be of interest to both management and auditors, who are responsible to implement and review controls, respectively. The article begins with some background information about Reg FD and how it can be fulfilled by using a corporate web site, before presenting the control issues.

Regulation Fair Disclosure

In the past, securities analysts played a significant role in obtaining material nonpublic information from firms, and then deciding how it was going to be disclosed to the public. From time to time, firms would disseminate up-to-date company information to a selected group of securities analysts and institutional investors through routes such as analyst meetings and investment conferences. Often, some of the released information would be material and nonpublic. Because most of these events were held in "closed-door" mode, retail investors (individuals investing for their own accounts) were excluded. When this practice of selective disclosure occurred, those who were privy to the material company information earlier were able to make a profit or avoid a loss at the expense of those kept in the dark. In addition, selective disclosure resulted in the loss of investor confidence in the integrity of capital markets.

To address the problem of selective disclosure, Reg FD attempts to "level the playing field" by ensuring that information is available to all interested parties on an equal-access basis. To put it briefly, Reg FD requires that when a firm, or person acting on its behalf, discloses material nonpublic information to a select group of people (normally securities market professionals and securities holders), the same information must also be disclosed to the public. The timing of the required public disclosure depends on whether the selective disclosure was intentional or unintentional.[2] For an intentional selective disclosure, a firm must make public disclosure simultaneously. For an unintentional disclosure, a firm must make public disclosure promptly.

Corporate Web Site for Information Disclosure

Reg FD does not recognize the Internet as the exclusive vehicle through which the public can be fairly informed.[3] Rather, Reg FD permits firms to make public disclosure by filing or furnishing a Form 8-K with the SEC or by disseminating information through another method (or combination of methods) of disclosure that is reasonably designed to provide broad, nonexclusive distribution of the information to the public.[4]

Some business professionals argue that no other routes can provide a better way to disseminate information to the public than the Internet, with respect to compliance with Reg FD.[5] Even if a firm holds an anachronistic telephone conference call, or issues an equivalently anachronistic press release to disclose company news, none of these routes is as accessible to the public as a corporate web site, which is available to anyone across the globe with an Internet connection.[6]

Through its corporate web site, a firm can ensure that all stakeholders, regardless of their geographical location, are simultaneously informed of company news (a timing issue). This is hardly possible using traditional communication channels such as mail and telephone calls. For this reason, many firms have implemented and utilized their corporate web sites for informal dissemination. For instance, the web site of the New York Stock Exchange (NYSE) has an investor relations section, containing material news such as the latest press releases and financial reports.

Besides the timing issue, ensuring that all the stakeholders receive exactly the same amount and format of information is another problem without the use of the Internet. For example, a listed firm organizes an exclusive conference for a group of selected securities analysts and institutional investors. Thereafter, the firm prepares and uploads a set of presentation slides or a PDF document to its corporate web site. In this situation, even though the firm claims that all the material information released in the conference can also be found on the corporate web site, retail investors may question the validity of such a claim. Today, this issue is no longer a problem, thanks to Internet technologies and webcasting in particular.

Webcasting

Webcasting, also known as cybercasting or Internet broadcasting, allows the content provider to use the Internet to broadcast live or delayed video/audio clips to geographically dispersed audiences in a cost-effective and user-friendly manner.[7] Webcasting allows people to "virtually" and conveniently attend live events, or watch previously recorded events via their personal computers (PCs).

To view a live or recorded event (e.g., an analyst briefing), people simply click on the provided webcast URL or the desired content item on the corporate web site. As such, webcast audiences can enjoy a "nonthreatening" (because they will not be seen or heard, and even when interaction features are used, the attendees can opt not to interact), high-impact session that includes, for example, streaming video, streaming audio, presentation slides, browser sessions, surveys and polling.[8] Generally speaking, for medium to large audiences, webcasting is far more cost-effective than audio or web conferencing.[9] Its innumerable benefits make webcasting an ideal means of corporate communication, especially in the distribution of rich-media information. Indeed, webcasting has raised the business use of the Internet to the next height.

Major Control Issues of Internet Corporate Reporting

However, Internet corporate reporting (ICR) (including webcasting) alone is insufficient, because it is not an "isolated island." Like other technologies, ICR is ultimately integrated into a larger, more complex social and technological organization such as a business firm.[10] Thus, simply adopting ICR does not guarantee an adequate compliance with Reg FD. Instead, adopting ICR in a firm must be well planned, managed and controlled in order to derive the maximum benefits from it.

Some of the major control issues that management and auditors should pay attention to when they manage or review ICR adoption in their firm include:

- **Types of reported information**—It has been well observed that investors with different backgrounds prefer different types of financial data.[11] More specifically, the types of financial data preferred by investors vary with their relative sophistication of financial knowledge. In general, professional stock analysts favor relatively objective, more extensive information, such as same-day or historical stock prices. On the other hand, retail investors (generally assumed to be less sophisticated financially) prefer relatively subjective, more abbreviated information, such as discussion of the advantages of owning a firm's stock, including management interpretation. Based on this observation, management and auditors should ensure that investors with different backgrounds are provided with the types of online information they prefer.
- **Formats of reported information**—Online company information can exist on a corporate web site in various formats, e.g., Hypertext Markup Language (HTML), PDF, presentation slides or spreadsheets. Thus, due attention must be paid to the formats of the information provided on the corporate web site. Because the ultimate purpose of the online information is to help the investors make their investment decisions, this information should be presented in a format (or a combination of formats) with this purpose in mind. In general, a PDF document containing financial information may suffice for most retail investors. On the other hand, professional stock analysts may prefer that financial information be presented in a spreadsheet format. Thus, the information can be imported into their investment software for detailed analysis.
- **Coverage, correctness and consistency of reported information**—Management/auditors should determine/evaluate the coverage of corporate information to be reported online. Some common types include annual reports, interim reports, annual or interim results, real-time share price movement, and historical dividends per share.[12] As a general guideline, management/auditors should ask themselves questions such as: Are these types of information adequate and sufficient for the variety of expected online visitors? If not, what else should be reported? How long should archived information be kept on the corporate web site?

  In addition, using extreme caution, all the online information provided on the corporate web site must be correct and precise as far as possible. Otherwise, investors may sue the firm for wrongfully disseminating incorrect and ambiguous information, resulting in their poor investment decisions. Furthermore, if the same piece of information appears more than once on the corporate web site (possibly in different formats such as video/audio clips, presentation slides and PDF documents), that information must be consistent throughout the entire web site. In any case, a disclaimer must be included on the corporate web site to reduce the risk of legal disputes about the content of the reported information.
- **Frequency and timeliness of reported information**—Besides the previous three Cs (that is, coverage, correctness and consistency), the frequency and timeliness of reported information is another consideration. In this regard, some important questions to be asked by management and auditors are: Should the interim results be reported on a quarterly or biannual basis? Should the annual report (which includes the auditor report) be provided online immediately after the completion of the annual audit exercise? How long should the financial performance data be posted to the corporate web site after the data have been released officially via the press or an analyst briefing (this last question is particularly relevant to compliance with the Reg FD)?
- **Accessibility of reported information**—From the investors' point of view, access to online information must be uncomplicated and user-friendly. Given today's high demand of the investors, providing a simple fool-proof navigation and alternative navigation paths to the same information item on a corporate web site is no longer an option; it is a must. Common questions in this aspect are: Is the financial information placed in the appropriate section on the corporate web site? How deep from the home page of the web site do visitors have to navigate to retrieve the relevant financial information? Are the web pages that contain the online financial information interconnected via hyperlinks?

- **Size and transmission speed of files containing corporate information**—Thoughtful consideration should be made to the size and transmission speed of the files containing corporate information, particularly for video/audio files, which are normally large in size. This issue becomes more important when the demand of online visitors and the traffic on the corporate web site grow with remarkable speed. An underpowered and sluggish web site will result undoubtedly in disillusioned online visitors.[13] Thus, it is essential that the platform used to host the web site can be scaled up when needed.
- **Compatibility and quality of video/audio clips**—If a firm adopts webcasting to provide rich-media information captured in video and audio clips, it is vitally important that these clips can be played back by most popular media player software, e.g., Microsoft Windows Media Player, RealPlayer. Furthermore, the image and sound qualities of such clips should be monitored to ensure that the amount of distortion and distraction is kept to an absolute minimum.
- **Languages of reporting**—Most (if not all) listed firms have an international base of shareholders and investors. Because of this reason, the online information (including video and audio clips) provided in the corporate web sites ideally should be multilingual to help investors overcome their language barriers. Consider, for instance, the listed firms in Hong Kong. Being an international city where "the East meets the West," both Chinese and English are very popular languages in the commercial sector. Thus, it is not surprising to see that, on the corporate web sites of most large firms listed in Hong Kong, the online information is presented in Chinese or English or both.

Conclusion

In today's dynamic and competitive business environment, ICR is no longer a "nice-to-have" option, but rather an essential and affordable one that any firm should implement for disseminating information to a global audience. ICR (including webcasting) also serves as an effective vehicle for fulfilling Reg FD. In light of the utmost importance of ICR, a corporate web site should not only be rich in content, but also facilitate online visitors to locate the corporate information they look for from the site by means of easy navigation. It will certainly be unwise for management, accounting, finance, IT staff or auditors of a firm to ignore ICR. Therefore, those people who are involved in the planning, design, implementation and review of ICR should have a good knowledge of the related control issues.

Endnotes

[1] Myers, L.; "Regulation FD and Private Trading on the Internet: Keeping Pace With Constant Change," *Journal of Legislation and Public Policy*, vol. 5, no. 1, 2001, p. 15-21. SNLSecurities, "Investor Relations and the Web," *www.snl.com/irweblink/IRWEB_final.pdf*

[2] US Securities and Exchange Commission (SEC), "Final Rule: Selective Disclosure and Insider Trading," USA, 15 August 2000, *www.sec.gov/rules/final/33-7881.htm*

[3] Schwartz, J.; "One Small Step for the Blogosphere," Jonathan's Blog, 2 October 2006, *http://blogs.sun.com/jonathan/entry/one_small_step_for_the*

[4] *Op cit,* US SEC 2000

[5] *Op cit,* Schwartz

[6] Hodge, D.; "Hyperlinking Unaudited Information to Audited Financial Statements: Effects on Investor Judgments," *The Accounting Review*, vol. 76, no. 4, 2001, p. 675-691. Oyelere, P.; F. Laswad; R. Fisher; "Determinants of Internet Financial Reporting by New Zealand Companies," *Journal of International Financial Management and Accounting*, vol. 14, no. 1, 2003, p. 26-63

[7] Mack, S.; D. Rayburn; *Hands-on Guide to Webcasting: Internet Event and AV Production*, Elsevier/Focal Press, USA, 2006. Paul, S.; *Multicasting on the Internet and Its Applications*, Kluwer Academic Publishers, USA, 1998

[8] Weinstein, I.M.; *Effective Enterprise Webcasting: Optimizing Your Webcasting Solution for Efficiency and Success,* Wainhouse Research, USA, 2005

[9] *Ibid.*

[10] Flor, N.V.; *Web Business Engineering: Using Offline Activities to Drive Internet Strategies*, Addison Wesley, USA, 2001. Poon, P. L.; A. H. L. Lau; "The Present B2C Implementation Framework," *Communications of the ACM*, vol. 49, no. 2, 2006, p. 96-103

[11] Ettredge, M.; V.J. Richardson; S. Scholz; "A Web Site Design Model for Financial Information," *Communications of the ACM*, vol. 44, no. 11, 2001, p. 51-55

[12] Lymer, A.; "The Use of the Internet for Corporate Reporting: A Discussion of the Issues and Survey of Current Usage in the UK," *Journal of Financial Information Systems*, 1997

[13] *Op cit*., Poon and Lau

Antonio Wong, Ph.D., CFA
is a lecturer at the School of Accounting and Finance of the Hong Kong Polytechnic University. His research interests include corporate finance and investments, and web-based financial systems. He was an *ad hoc* reviewer of the *China Accounting and Finance Review* journal. He can be reached at *afcpwong@inet.polyu.edu.hk*.

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 corecipient 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*.

Solving the Puzzle of IT for Sarbanes-Oxley:

IT's Role in Sarbanes-Oxley Compliance

By Paul Rozek

Sudoku puzzles have more in common with the Sarbanes-Oxley Act than one might think. The logic-based puzzle, created by Nikoli Co. Ltd. of Japan, is about strategy and analysis, and can be daunting when first attempted. Once a strategy is developed, a player can work through multiple levels of difficulty using the established tactics as a guide.

When it became clear that IT would play an important role in public company compliance of Sarbanes-Oxley, the IT sector had to start from scratch to develop a compliance strategy, i.e., a control framework that would become standard practice for all IT managers. The overall feeling was similar to a person trying to solve a Sudoku puzzle for the first time: the information had to add up, but the trick was finding the most efficient way to assess the IT controls associated with financial data integrity.

Achieve business advantages through efficient and effective operations.

Now, six years later, IT managers have a better understanding of how to recognize common IT controls through the IT Governance Institute (ITGI)'s *IT Control Objectives for Sarbanes-Oxley* publication.[1] This document offers potential methods to identify whether such controls have been operating effectively over time. In fact, the work required to meet the requirements of Sarbanes-Oxley is no longer being regarded as a compliance process, but instead as an opportunity to establish a strong governance model designed to ensure accountability and responsiveness. It is possible to harness the power of IT governance to develop controls for financial reporting and data retention that will be successful year after year. IT managers just needed a consistent plan to solve the puzzle.

Developing a Strategy

An overarching IT control program should enhance overall IT governance; improve the understanding of IT among senior executives; promote better business decisions; align business and IT project initiatives; reduce IT risks, such as losing intellectual assets or falling victim to security breaches; contribute to the compliance of other regulatory requirements; and achieve business advantages through efficient and effective operations.

IT management needs to perform five steps in documenting its internal controls to support IT Sarbanes-Oxley compliance requirements. A well-defined documentation flowchart, naming standards that enable cross-referencing of documentation for internal personnel and external auditors, is vital to the success of the IT Sarbanes-Oxley project.

Step 1: Determine the Scope

Scoping involves determining the documentation necessary and the extent of controls testing to be performed for significant accounts and business processes at each of the company's locations. Scoping is one of the most critical phases in the annual IT Sarbanes-Oxley project. During this phase, IT management will identify the significant accounts, disclosures and components, business processes/cycles and subprocesses/subcycles, and locations that will be subject to review.

IT management is required to base its assessment of the effectiveness of the company's internal controls over financial reporting on a suitable, recognized control framework. At this time, the ITGI framework found in the *IT Control Objectives for Sarbanes-Oxley* publication is one of the most widely applied models for IT Sarbanes-Oxley initiatives.

It is also important that IT management implement an annual process for reassessing its initial scoping decisions to ensure that they are updated appropriately for significant business and technology changes. Because scoping decisions typically are made early in the annual process, it is common for certain aspects of those decisions to change within the current year.

Step 2: Develop Process Control Narrative Documentation

IT management's documentation of processes will cover more than just the controls it plans to test. Documentation should enable IT management to understand the control processes from start to finish, and cover the initiation, authorization, recording, processing and reporting of individual high-risk transactions. For example, IT management will document the entire change control process, from the initial request through the move into production. Without such documentation, it would be difficult to identify points in the process where a potential error or fraud could occur. It also would be difficult to determine the controls required to cover information processing objectives. In addition, change control processes may vary by system, application or database. Accordingly, IT management should document each of those different processes for Sarbanes-Oxley purposes.

Documentation of processes may take various forms: flowcharts, policy manuals, accounting manuals, narrative memoranda, decision tables, procedural write-ups and completed questionnaires. No single form of documentation is required, and the extent of documentation varies depending on the company's size and complexity. However, narrative descriptions supplemented by flowcharts are frequently the most effective form of process documentation. The volume of data in the narratives is not as important as documenting the applicability and clarity of the control processes to support financial data integrity.

Step 3: Develop Risk/Control Matrix Documentation

Once IT management has documented the in-scope processes, it should document the design of the controls that are relevant to financial reporting. This documentation enables IT management to assess whether the controls cover the financial statement assertions that were mapped during the scoping phase. In assessing the design of the controls, IT management must determine whether the controls (i.e., procedures, processes, policies, systems) will, if operating as intended, provide reasonable assurance that IT management's control objectives are being met *vis-a-vis* the relevant financial statement assertions for all significant accounts and disclosures. This is often referred to as design effectiveness.

The ITGI framework is one of the most widely applied models for IT Sarbanes-Oxley initiatives.

IT management will evaluate the operating effectiveness of controls during the testing phase of the project. However, if the design of a control is flawed, the company will not achieve the desired assurance that the control is capable of preventing or detect a misstatement even if the control is operating as intended. IT management will then need to remedy design deficiencies.

Step 4: Assess the Design and Operational Effectiveness of Controls

After IT management has documented the design of the controls for in-scope processes, it should determine the effectiveness of the controls' design and which controls will be tested for operating effectiveness. These two events are closely linked. During the assessment of the design of controls, it should be determined whether the system of internal control is designed to suitably prevent or detect material misstatements on a timely basis. This evaluation should cover pervasive IT general controls and specific transaction-level control activities related to all relevant assertions for all in-scope processes and applications. Not all controls provide the same level of assurance.

In evaluating the level of assurance provided by a given control, IT management should consider the nature of the control, how the control is applied, the consistency with which it is applied and who applies it. While testing the operational effectiveness of controls, IT management will first determine and document which controls will be tested for operating effectiveness. As indicated previously, this determination naturally will be tied to the assessment of design effectiveness. Once again, this will require considerable judgment, and there is no quantitative formula or prescriptive checklist to follow.

IT management should test controls for all relevant financial statement assertions for all systems, applications and databases that impact significant accounts and disclosures for all individually important locations and significant specific risks. Although one control may cover a specific assertion, the ITGI publication indicates that a combination of preventive and detective controls is generally most effective. The controls that are to be tested typically are designated as key controls. Some companies use a rating scheme (i.e., high/medium/low) to define the degree of assurance a control provides. A company may plan, for instance, to test only the high- and medium-rated controls. A high level of assurance that controls are working effectively is required. No single scheme is necessarily correct. For simplicity, controls that ultimately will be tested for operating effectiveness are identified as key controls.

In general, controls are tested on an accept/reject basis, meaning a control is either working reliably or it is not. To attain a high level of assurance regarding the operating effectiveness of a control, no more than a negligible exception rate can be accepted. If an exception occurs in testing, IT management must evaluate the exception to determine why it occurred. Upon investigation of the exception, IT management may determine that the control is not operating effectively. Alternatively, the results of the investigation may not find conclusively that a deficiency exists. In this circumstance, assuming the control operates at least daily, IT management may select and test another sample of equal size. If no exceptions exist in the second sample, a conclusion that the overall exception rate is no more than negligible would be appropriate. In this case, the exception would not be considered a deficiency as the likelihood of misstatement is not high. It is critical for IT management to work closely with its external auditors to clearly communicate what constitutes an exception and what level of testing is required to "prove" that a remediated control is now working effectively.

Step 5: Finalize the Summary of an Aggregated Deficiencies Chart

IT management should finalize the inventory of all internal control deficiencies, significant deficiencies and material weaknesses. The root cause for each deficiency should be documented, and an assessment of the necessary corrective actions should be made. The project leaders and/or steering committee should carefully assess each deficiency and prioritize remedial actions. Each remediated control should be retested to verify its operating effectiveness. A summary of aggregated deficiencies (SAD) document can also provide IT management with a historical view of issues that were uncovered in the past and the successes associated with the remediation activities.

Solving the Puzzle

The IT Sarbanes-Oxley process provides a tremendous opportunity for the internal IT auditor to be recognized as an internal controls consultant. As control experts, IT auditors can help their firms mitigate risk by recommending ways to enhance existing IT governance activities and ensuring the IT Sarbanes-Oxley program is integrated successfully into the culture of the enterprise.

Multiple areas of IT that do not directly affect financial data integrity must be reviewed. For example, there are many non-Sarbanes-Oxley applications that may have a significant impact on the effectiveness and efficiency of business operations. Technical vulnerability assessments that assess networks, databases, Internet applications, servers and more should be performed regularly. Compliance with regulations, such as the US Health Insurance Portability and Accountability Act or the Payment Card Industry Data Security Standard, are typically segregated from IT Sarbanes-Oxley controls. However, there is substantial interest in attempting to create a one-test-tests-all approach with respect to compliance controls.

Just like the Sudoku puzzle, there is more than one process that will correctly solve the annual IT Sarbanes-Oxley process. There are too many examples of firms not making a sufficient effort to identify and fix the root causes of compliance deficiencies within their IT functions. By not having formal remediation action plans to fix such issues in a timely manner, enterprises can create significant ripple effects on future years' reporting.

Following a governance-oriented process for IT Sarbanes-Oxley can reduce the time, expense and remediation pain of improper disclosure. A repeatable process will also increase reliance of external auditors on an enterprise controls architecture, enhance controls awareness throughout the firm and enable implementation of continuous controls monitoring programs—especially those that enhance the management of evidence of operational controls' effectiveness. With diligence, and a sharp eye to project planning and managing the level of detail, the IT Sarbanes-Oxley puzzle can be solved.

Endnotes

[1] IT Governance Institute, *IT Control Objectives for Sarbanes-Oxley, 2nd Edition*, USA, 2006, *www.itgi.org*

Paul Rozek

is director of technology risk management services with the Wisconsin, USA, offices of Jefferson Wells (*www.jeffersonwells.com*). He is responsible for the office's strategic direction, staffing and delivery of professional services related to IT auditing, information security, business continuity and IT governance. He can be reached at *paul.rozek@jeffersonwells.com*.

FEATURE

Electronically Stored Information and Cyberforensics

By Albert J. Marcella Jr., Ph.D., CISA

A New Age of Discovery

The US Sarbanes-Oxley Act, US Health Insurance Portability and Accountability Act, US Gramm-Leach-Bliley Act, Basel II, and the International Organization for Standardization's ISO 17799 and ISO 27000—has it been a struggle to comply with these guidelines and implement internal control standards? Well, it is not getting any easier.

While the noncompete, nondisclosure, acceptable-use and rights management policies had seemed difficult to articulate and then implement, those may soon seem like the halcyon days. The next set of policies is expected to be even tougher to define and implement. In addition, failure to do so will no longer be looked at as an outstanding noncompliance item in an audit report.

In the US, the world of records retention and content management, as most industry professionals knew it, was retooled on 1 December 2006, with the official enactment of the new amendments to the US court system's Federal Rules of Civil Procedure (FRCP). Those rules now require any business that may find itself involved in litigation in US federal court to retain and manage electronic records.

The term "electronically stored information" (ESI) is applied to today's vast array of electronically generated documents, encompassing more than storage and retention, while ensuring that ESI generated by an enterprise is secure and protected from unauthorized access, use or destruction.

Federal Rules of Civil Procedure

Electronic discovery in legal matters is a complex issue that cannot be ignored. Consider the massive volume of enterprise data located in file systems, applications, preprimary storage and archives, and then recognize that it may be, at any time, discoverable. The new US rulesmerely underline what was already known: as ESI has become the norm, these records must be made available in the course of litigation. These new rules make this mandatory and require organizational discovery processesto be redesigned.

The new rules require that company attorneys and IT managers be able to demonstrate how ESI is stored; the procedures established to manage, control, protect and retrieve them under court order; and the policies governing their retention. In addition, the new rules require evidence of an established history and implemented routine for the deletion of corporate ESI. Feigned ignorance and plausible denial are matters that may have satisfied judicial inquiry in the past, but they are no longer tolerated by US courts. Noncompliance risks the most serious of consequences. In 2005, the Alabama (USA) Circuit Court of Appeals fined General Motors US $700,000 for delaying a discovery process by 98 days.

Legal Impact

Surveys completed by several organizations clearly show that a large percentage of corporations are either unaware of this new federal ruling and its impact on their day-to-day operations or, if they are aware, they are underprepared to comply should they be compelled to do so. For example:

- In a Cohasset Associates survey, nearly 50 percent of respondent organizations have no e-mail retention policy in place.[1]
- The ability to handle difficult e-discovery matters is a source of concern for most enterprises surveyed by law firm Fulbright & Jaworski. Just 19 percent of respondents consider their companies to be "well prepared" for e-discovery issues, while the vast majority (81 percent) report being "not at all" to "somewhat" prepared. More than a third of the UK contingent (35 percent) feel "not at all" or "poorly" prepared, while 23 percent of the US respondents fall into this category. Even the largest companies demonstrate little confidence in their preparedness, with just 19 percent feeling well prepared. No one reported feeling completely prepared.[2]

ESI As Evidence

A significant difference exists between the US criminal and civil court systems. The chief difference is that in a civil case, the victim controls essential decisions shaping the case. It is the victim who decides whether to sue, accept a settlement offer or go to trial.

In the civil justice system, liability must be proven by a preponderance of the evidence, which simply means that one side's evidence is more persuasive than the other's. In other words, the plaintiff must prove there is a 51 percent or greater chance that the defendant committed all the elements of the particular wrong. This standard is far lower than the "proof beyond a reasonable doubt" required for a conviction in the US criminal justice system.

It may not be a case of "if" but more realistically "when" this fact will compel enterprises to take a hard look at their ability to identify, retrieve and produce requisite ESI.

An enterprise must ask itself or, better yet, ask its senior management what the likelihood is that it will face the need to produce ESI and whether the enterprise is prepared to respond within mandated time frames.

Additional findings from the Fulbright & Jaworski survey indicate that large companies (more than US $1 billion in annual revenue) face an average of 556 lawsuits worldwide and spend an average of US $34 million on legal costs. The survey of 422 members of in-house counsels also found that 89 percent of respondents reported at least one new suit filed against their company in the past year.[3]

Today's reality is that "93 percent of all business documents are created electronically."[4] When coupled with the decreasing cost of storage, this allows "[t]oday's 'digital packrat' [to] hoard astronomical quantities of electronic information. …According to a recent article in the *Wall Street Journal*, 'We went through a belief that storage was cheap so we could save everything'…[and] although storage may be cheap or free,…it is not necessarily the wisest decision for an organization to make."[5]

Laura Bandrowsky, chief operating officer of Wescott Technology Services LLC, cautions, "The volume of data that must be managed or handled for litigation directly affects the cost of discovery."[6]

In the eventuality of e-discovery, cost containment is the challenge.

Hold Management and Spoliation

Two important concepts related to ESI are hold management and spoliation.

Hold management refers to the ability to respond to a legal action. Once an enterprise is notified of a legal action, all records that may relate to that action are placed on legal hold. They may not be destroyed and their profile information may not be modified. They must be prevented from destruction until the hold is lifted. The ability to hold records may also be applied to audit situations when required.[7]

Loss or destruction of evidence exposes litigants to drastic monetary, evidentiary, criminal and other sanctions, including, in some jurisdictions, liability for the tort of spoliation.[8]

Spoliation of evidence refers to the willful destruction of evidence that is germane to the case in litigation. This would include destruction of ESI. However, given the volume of electronic documents created in virtually every business today, it is usually necessary to delete, archive and/or overwrite documents in the routine and normal course of business. Accordingly, many companies have data management systems and/or data retention policies in place, which include deletion of ESI on a regular basis.

Spoliators of evidence in legal actions are individuals who neglect to produce evidence that is in their possession or control. In such a situation, any inferences that might be drawn against the party are permitted, and the withholding of evidence is attributed to the party's presumed knowledge that it would have served to operate against him/her.[9]

Safe Harbor

Section 26(f) of the FRCP provides for a safe harbor against sanctions being imposed in the event of electronic information that might be lost under the "routine, good faith operation" of such a data management system or data retention policy. It is important to remember, however, that this amendment does not provide a shield for any party "that intentionally destroys specific information due to its relationship to litigation or for a party that allows such information to be destroyed in order to make it unavailable in discovery by exploiting the routine operation of an information system."[10]

Figure 1 summarizes the expected impact of the new amendments on an enterprise's IT policies and procedures. The auditor is advised to assess these changes with respect to the impact that they may have on the auditor's internal IT practices and policies.

Figure 1—Impact of New US Amendments

Amendment	Effect on IT
Rule 16(b): A description of all electronically stored information must be presented within 99 days of the beginning of a legal case.	E-mail archiving, retention software and policies should be put in place.
Rule 26(a): Electronically stored information, including e-mail, must be searched without waiting for a discovery request.	E-mail archiving and retention policies should be put in place by IT so information can be discovered rapidly.
Rule 26(b): A party need not provide discovery of electronically stored information if there is an undue burden or cost.	The enterprise is required to prove that installation of e-mail archiving software is an onerous expense.
Rule 26(f): Litigants are required to discuss any issues relating to preserving discoverable information.	Legal counsel is required to know how e-mails are being retained and how they can be searched and retrieved.
Rule 34(b): The requesting party is required to designate the form in which it wants ESI to be produced; the responding party is required to identify the form in which records will be produced.	IT must be aware of how e-mails are stored, e.g., on disk or tape, and how they will be retrieved.
Rule 37: A safe harbor provision for deleting records must be established.	IT may establish policies for the deletion of e-mail.

Moving Forward With ESI

Given the volume and variety of communications that pass through an enterprise on any given day, the absolute necessity for a viable, well-thought-out, well-planned and well-tested document management program is essential to the survival of the 21st century corporation. Add to that the legislatively mandated requirement that any business that may find itself involved in litigation in US federal court must have procedures in place to retain and manage electronic records, and the motivation for a document management program goes from a need to a business requirement.

Identifying exactly which corporate communications must be retained and then establishing the appropriate procedures to do so takes time, energy, effort and financial resources. Assessment by the enterprise's internal audit function or review by an external third party must be built into the overall program to ensure compliance and corporate readiness.

Weaknesses in the enterprise's document management program must be corrected, and appropriate controls that endeavor to maintain a compliant document management program and provide management with the information resources necessary to respond effectively, appropriately and in a timely manner to a court order requiring the enterprise to produce ESI must be implemented.

Global Perspective

While the FRCP and its application to ESI, as noted previously, is US-centric in its application, these principles, along with the recommendations presented for implementing vigilant internal controls, are truly global in their implication and application. Enterprises that may never anticipate stepping foot into a US federal court can benefit greatly from an assessment of their current document management procedures and subsequent implementation of a well-designed strategy to control organizational ESI. They benefit by achieving an overall better-controlled records management and retention process, having an ability to identify critical ESI, establishing retention and destruction cycles and access rights, and ultimately being better prepared to meet the potential for similar emerging legislation in their own countries.

Auditing ESI Preparedness

As regulators and courts increasingly recognize the enhanced and richer information value of electronic data compared with physical documents, companies should strengthen their ability to safeguard their rights and respond appropriately.[11]

The points, actions and activities provided in the sidebar, "ESI Audit Considerations," should be examined as potential recommendations to management. These practices may be implemented to establish an enterprisewide, proactive document management program that addresses the issues of compliance and governance, assists in mitigating potential legal culpability, and establishes solid internal controls for corporate ESI.

ESI Audit Considerations

1. Have a plan and a process for discovery of ESI that can improve over time.
2. Understand the end-to-end process from discovery to production and the implementation of "holds." This encompasses methods and practices that make sense for the enterprise, understanding where technology is needed to facilitate or improve process efficiencies or quality of results, and identifying the specific technology capabilities that are required to make the end-to-end process effective. It is best accomplished through a cooperative effort among legal, IT and the line-of-business (LOB) organizations.
3. Consider technology capabilities such as dedicated computer storage and processing resources with robust security, inventory and identification of ESI sources potentially relevant to the request.
4. Examine search and retrieval tools that can be responsive to the request and are robust enough to deliver results in tight time frames, with the appropriate degree of precision.
5. Consider integrated content management, which provides "middleware" to link multiple sources of ESI for search, retrieval and possible collection, if there are multiple content sources.
6. Conduct benchmarks to test and establish parameters for various electronic discovery scenarios. Repeatable processes that have been tested to provide evidence of results of sought-after records production for a given set of metrics can be a significant key to negotiating e-discovery requests. This will help effectively plan the response activities and time frame and prudently apply resources and budget.
7. Develop repeatable processes that have the flexibility to accommodate a variety of discovery and regulatory requests.
8. Develop and implement records management and retention policies that can effectively preclude retaining nonmaterial information. Formal guidance to promote the appropriate and prompt disposal of unneeded ESI is an important component of records management.
9. Maintain an inventory of ESI sources that documents system descriptions and characterizations, such as computing system and location, software product and version, business purpose and scope, data storage (active drives or archives), retention location and periods for backup data, estimated volume of data being retained, and native capabilities for search and data formats. This inventory provides auditors and legal counsel with the data needed to estimate electronic discovery time and costs and determine an efficient and reasonable approach to develop the body of material for legal review.
10. Implement an ESI records management program that controls the volume of information through appropriate and regular destruction of ESI in the normal course of business.
11. In addition to establishing and implementing destruction policies through the records management program, provide the mechanisms and protocols to suspend destruction for the specific ESI required to comply with discovery and preservation orders.
12. Keep pace with changing regulations, new requirements and trends in enforcement.
13. Have a process whereby compliance or regulatory affairs, or whatever entity has the responsibility to monitor regulatory initiatives and implement compliance measures for new regulations, communicates the requirements across the enterprise. These communications include, for example, legal, technologies, risk management, records management, audit and relevant LOB management.
14. Reach an understanding of the potential impact of legislation such as Sarbanes-Oxley and Basel II (financial services) on requirements for controls and audit trails across intraorganizational boundaries.
15. Review and appropriately update, in a timely manner, records management mechanisms, technologies and protocols for retention and destruction.
16. To avoid increasing risk and costs of noncompliance, do not just update the records retention and management program, but completely overhaul it. This requires

knowledge of electronic records, records management, ESI technology issues and characteristics, and the total information fabric of the business that encompasses information in all forms.

17. Create an effective records management program for ESI. This considerably reduces volumes of physical material held in storage and significantly decreases discovery efforts and production of physical records.
18. Effectively use electronic discovery and search tools, and establish a consistent team with appropriate skills in electronic discovery and knowledge of the company's ESI sources, technology platforms and tools.
19. Establish a set of tools that can provide predictable results based on established protocols.
20. Periodically conduct benchmarking exercises against a variety of ESI sources to establish metrics using the enterprise's tools of choice. These metrics help to establish the time frames and costs of searching various electronic source systems using various scenarios and parameters. For example, how long does it take to search and report results on 20 named individuals in the enterprise's e-mail system regarding one matter over a period of three years?
21. Understand the metrics and time requirements for simple search, de-duping and creation of "collection" stage files, separate from the time and effort required for legal or other reviews, advanced searching, and culling of irrelevant or privileged information. Conduct the benchmarking on current systems, retired systems and archive systems.
22. Implement hold management rules (prelitigation identification of potentially material information and ongoing implementation of document preservation orders) that require special attention and tools for ESI. The rules that will determine which ESI are to be held (beyond their scheduled retention period) require careful crafting (by legal counsel, perhaps with assistance from IT and LOB managers) and an analysis of holdings in the context of ESI and business systems. A lack of a clearly defined "registry" for records (such as what can be provided by a document management or records management system) to which the rules can then be applied constrains adoption of automated techniques and can lead to an outcome that all ESI is "on hold forever."
23. Consider the information fabric of the enterprise and create policy-based rules for managing ESI that not only facilitate discovery and document production activities, but yield business benefits as well. Defining and incorporating records life-cycle-based controls and retrieval protocols also facilitate meeting trustworthiness and authenticity requirements.
24. Make retention decisions in the context of what the data represent, where they reside, longevity of preservation and vitality of systems.
25. Evaluate systems (sources of ESI) and determine how older information might be accessed reasonably. If it cannot be accessed reasonably, critically examine why it is being retained.
26. Implement policies and records-destruction practices in accordance with documented protocols that become part of the normal course of business.
27. Update IT governance practices to include identification of retention requirements (based on legal, regulatory or other factors) in the design requirements for new systems.
28. Consider the impact of encryption policies on search and retrieval capabilities. With the increasing adoption of encryption for e-mail and attachments, there are concerns that e-mail will not be searchable because of "loss" of the appropriate encryption keys, introducing further complexity to maintain accessibility of aging ESI. ESI that is subject to production, but cannot be decrypted, could result in raising suspicions of spoliation.
29. Consider the impact of destruction methods and available technology.
30. Multiple regulatory requirements can pertain to any particular class of ESI. Therefore, when there are changes in any particular regulation affecting records, evaluate the impact of that change on the retention policy in consideration of other requirements that might apply.
31. Establish standard practices (automated where feasible) for regular destruction of ESI (e.g., on a monthly or quarterly basis) that are not unduly burdensome on employees. Establish communications and oversight practices that reinforce awareness and promote compliance. Destroy ESI as soon as possible, on a regular and consistent basis, and use methods that promote security and privacy for the information being destroyed.
32. Because many retention periods are triggered by an event, determine an event notification to the records management system to trigger the start of a defined retention time period. Any ESI that is on hold would have the retention period trigger set "on" when the event has occurred, but would not be destroyed until two conditions are met: the "hold" was lifted and the retention period has expired.
33. Establish basic metadata to be maintained as part of the record for each class of ESI, and implement metadata standards.
34. Identify audit trail requirements when developing metadata standards. If there are requirements for traceability and chain of custody, e.g., capturing (as metadata) who did what and when they did it, make them part of the metadata standard.
35. Ensure that the legal team is armed with an understanding of what ESI is or what is not accessible before entering electronic discovery negotiations.

Endnotes

[1] Connor, D.; “New E-Records Rules: Who’s Complying?,” *Network World*, vol. 23, iss. 47, 4 December 2006, p. 16

[2] Fulbright & Jaworski, “Third Annual Litigation Trends Survey Findings,” USA, *www.fullbright.com*, October 2006

[3] *Ibid*.

[4] Lange, M. C. S.; “E is for Evidence: Using an Online Repository to Review and Produce Electronic Data,” *Journal of Internet Law*, vol. 6, iss. 12, p. 18-21, June 2003

[5] Myler, Ellie; “The ABC’s of Records Retention Schedule Development,” *E-DOL*, May-June 2006

[6] Garretson, R.; “A Lifecycle of Its Own,” *CIO Insight*, iss. 76, December, 2006, p. 81-89

[7] *www.cmswatch.com/GlossaryTerm/137*

[8] Collins, C.; “California Eliminates Intentional Spoliation Tort,” Thelen Reid & Priest LLP, 21 July 1999, *www.thelenreid.com/index.cfm?section=articles&function=ViewArticle&articleID=1088*

[9] The Gale Group Inc., *West’s Encyclopedia of American Law*, “Spoliation,” 1998, *www.answers.com/topic/spoliation*

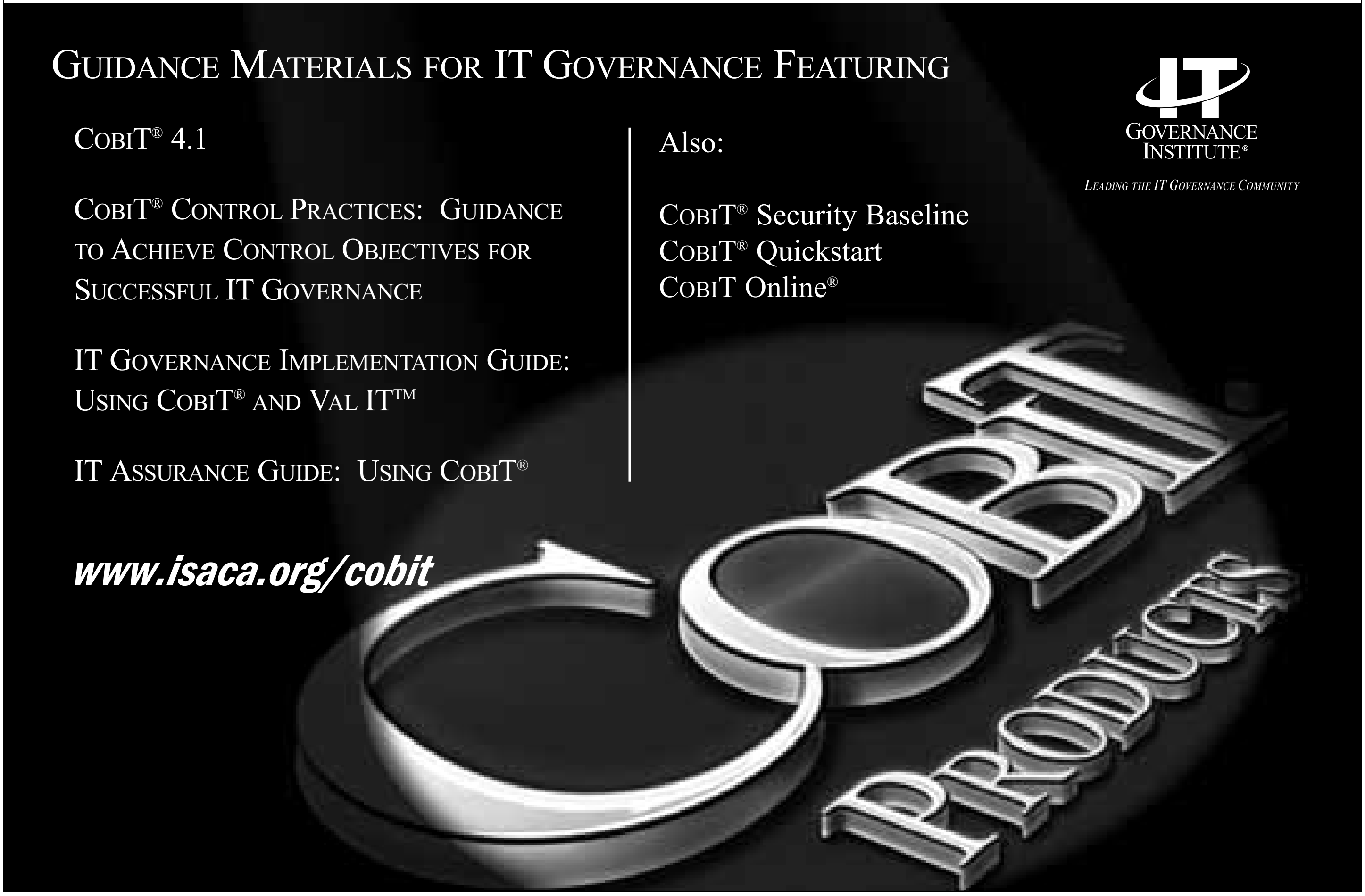
[10] Cortese Jr., A. W.; “Proposed Amendments to the Federal Civil Rules Strike a Healthy Balance,” *Defense Counsel Journal*, vol. 72, iss. 4, October 2005, p. 354-361

[11] Churchill, B., et al.; “The Impact of Electronically Stored Information on Corporate Legal and Compliance Management: An IBM Point of View,” IBM Corp., USA, October 2006 (used with permission), *www-03.ibm.com/industries/financialservices/doc/content/bin/fss_the_impact_of_eletronically.pdf*

Author’s Note

This article is based on the author’s recent book *Cyber Forensics II: A Field Manual for Collecting, Examining, and Preserving Evidence of Computer Crimes, 2nd Edition*, and excerpts are reprinted with permission of the publisher Taylor & Francis Group.

Albert J. Marcella Jr., Ph.D., CISA
is president of Business Automation Consultants LLC, a global IT and management consulting firm. Marcella is an internationally recognized public speaker, researcher, and workshop and seminar leader with 30 years of experience in IT audit, security and assessing internal controls. He is the author of numerous articles and 28 books on various IT-, audit- and security-related subjects.



Payment Card Industry Data Security Standard in the Real World

By Doug Drew, CISSP, PCI QSA, and Sushila Nair, CISA, CISSP, BS 7799 LA, PCI QSA

In response to growing concern about the misuse of stored information about credit and debit cards, the four major card-issuing bodies took steps to regulate the payment card-industry through the introduction of strict security procedures that govern how cardholder data are stored, processed and transmitted. Now collectively referred to as the Payment Card Industry (PCI) Data Security Standard (DSS), all member organizations that issue or acquire information from cards labeled with the Visa, MasterCard, American Express and Discover logos are required to comply with the requirements for auditing, scanning and assessment outlined in PCI DSS. While the common standard simplified the process that card issuers and acquirers were subjected to originally—no longer were they required to follow up to four separate programs applied differently in each region or country of operation—the new PCI DSS has introduced its own set of complexities.

How PCI DSS Works

PCI DSS originally began as four different programs: Visa's Card Information Security Program, MasterCard's Site Data Protection, American Express's Data Security Operating Policy, and Discover's Information and Compliance. Each company's intention was roughly similar: to create an additional level of protection for customers by ensuring that merchants meet minimum levels of security when they store, process and transmit cardholder data.

In December 2007, the four card issuers aligned their individual policies to create one overarching standard: PCI DSS. The standard sets forth common requirements for auditing, scanning and assessment, which ensure that vendors do not have to go through multiple programs to make certain that their environments comply with each individual card company's standards. The standard also provides a common implementation schedule, levels and participation criteria for merchants and service providers, as well as cross-recognition of qualified onsite assessors and compliant scanning vendors in Canada, Europe and the US.

PCI is made up of member organizations, which are classified as acquirers and issuers, and a few select players who perform both functions. While the terminology is somewhat arcane, the basic distinction is that acquirers handle the merchants that conduct transactions, while issuers are responsible for the issuing of cards to cardholders. A final group—service providers—are the entities that provide any service requiring the processing, storing or transportation of card information at the request of either acquirers or issuers.

Figure 1—Merchant PCI DSS Levels (Visa's Definition)

Level	Transactions
Level 1	• Merchants with more than 6 million annual transactions (all channels) • All third-party processors (TPPs) • All data storage entities (DSEs) storing data for Level 1, 2 and 3 • All compromised merchants, TPPs and DSEs
Level 2	Any merchant, regardless of acceptance, channel-processing 1 million to 6 million transactions per year
Level 3	Merchants with more than 20,000 annual e-commerce transactions
Level 4	All other merchants

The PCI Security Standards Council (PCICo) sets the high-level requirements, but each card association implements and enforces the standard, fines/fees, and compliance levels and deadlines. Despite being a global standard, PCI DSS is subject to minor variations based on both the card association and, in the case of Visa, physical location. The most notable difference is that MasterCard implements its programs globally, but Visa implements PCI DSS on a regional level, in keeping with its overall business, and this results in small variations. For example, level 1 merchants in the US can perform their onsite audit with the use of internal audit staff instead of using a Qualified Security Assessor (QSA), as long as they have the report on compliance (RoC) authorized by an officer of the corporation. This is not an option in Asia-Pacific because of different corporate governance issues there.

PCI DSS uses levels to determine compliance validation requirements. For merchants (**figure 1**), their level is determined primarily by the volume of credit card transactions performed, but a history of data breaches can force smaller merchants into the top tier. All service providers that are credit card processors or payment gateways are level 1; level 2 and level 3 are service providers that do not fall into this category, determined by the volume of cards processed as displayed in **figure 2**. The levels are card-specific and differ for each card company. In the case of Visa, which operates regionally, there are differences in the levels according to geographic region. Merchants should always contact their acquirer to determine their level.

Regardless of the level in which a service provider or merchant falls, it does not impact the requirements—they are the same across all levels. The level impacts only the validation requirements.

Figure 2—Service Provider PCI DSS Levels

Level	Transactions
Level 1	All processors and payment gateways
Level 2	Any service provider that is not at level 1 and stores, processes or transmits more than 1 million credit card transactions/year
Level 3	Any service provider that is not at level 1 and stores, processes or transmits fewer than 1 million credit card transactions/year

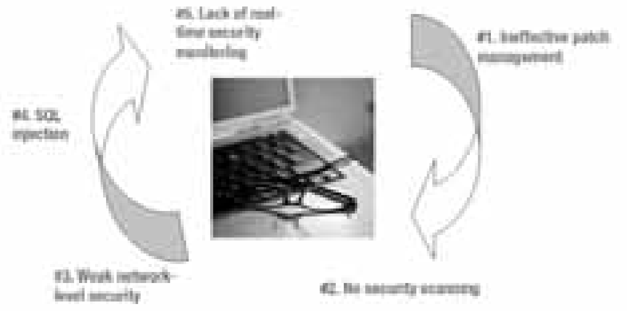
The most stringent validation requirements are reserved for level 1 and 2 service providers and for level 1 merchants. Providers and merchants in these levels must meet the DSS, conduct and pass an annual penetration test, conduct quarterly scans, and complete and pass an annual audit using external auditors. For level 2 and 3 merchants, the formal external audit requirement is replaced with an annual self-assessment, which must be approved by a qualified QSA. For level 4 merchants, all requirements, except meeting the DSS, are listed as optional. However, even at this level, failure to protect data adequately, as demonstrated by breaches or other data compromises, will result in the merchant's immediate "elevation" to level 1 status.

The PCICo manages the DSS, but it does not specify what the result of a failure to comply will involve. The individual card companies are responsible for setting those rules, and penalties can range from fines to suspension of the ability to accept credit cards. In the case of the card company having agreements with the acquirer rather than the merchant, the acquirer will be held responsible for a security breach within its mechant community. Acquirers are able to pass on these penalties to the offending merchant or service provider through their contractual relationships.

The requirements for each level are shown in **figure 3**. The asterisk denotes that this requirement is at the acquirer's discretion.

The requirements for PCI DSS are based on security breach analysis done by the card companies. The requirements, therefore, are based on real-world security analysis and, when implemented properly, should ensure that a company is secured against the most common types of attacks. **Figure 4** describes the top five reasons for account data compromise, according to MasterCard forensics analysis post-incident.

Figure 4—Top Five Reasons for Account Data Compromises


#5. Lack of real-time security monitoring
#1. Ineffective patch management
#4. SQL injection
#3. Weak network-level security
#2. No security scanning

Source: MasterCard

PCI DSS Requirements

To be compliant with PCI DSS, all enterprises must meet 12 requirements. While these requirements appear to be straightforward on the surface, they map to in excess of 200 subrequirements as outlined in the PCI Security Audit Procedures.[1] The 12 basic requirements are as follows:

1. Install and maintain a firewall configuration to protect cardholder data.
2. Do not use vendor-supplied defaults for system passwords and other security parameters.
3. Protect stored cardholder data.
4. Encrypt transmission of cardholder data across open, public networks.
5. Use and regularly update antivirus software.
6. Develop and maintain secure systems and applications.
7. Restrict access to cardholder data by business on a need-to-know basis.
8. Assign a unique ID to each person with computer access.
9. Restrict physical access to cardholder data.
10. Track and monitor all access to network resources and cardholder data.
11. Regularly test security systems and processes.
12. Maintain a policy that addresses information security.

The PCI DSS security requirements apply to all system components. A system component is defined as any network component, server or application that is included in, or connected to, the cardholder data environment. The cardholder data environment is that part of the network that possesses cardholder data or sensitive authentication data. Network components include, but are not limited to, firewalls, switches, routers, wireless access points, network appliances and other security appliances. Server types include, but are not limited to,

Figure 3—PCI DSS Requirements for Each Level

Category/Level	Meet the DSS Standard	Annual Audit	Annual Self-assessment	Annual Penetration Test	Quarterly Scanning
Service provider level 1	X	X		X	X
Service provider level 2	X	X		X	X
Merchant level 1	X	X		X	X
Merchant level 2	X		X	X	X
Merchant level 3	X		X		X
Merchant level 4	X	*	*	*	*

web, database, authentication, mail, proxy, Network Time Protocol (NTP) and Domain Name Server (DNS). Applications include all purchased and custom applications, including internal and external (Internet) applications. The scope of PCI DSS encompasses all systems that process, store or transmit cardholder information, as well as other systems that are in the same network zone. PCI DSS defines network zones as all systems that share a common boundary. Network zones are separated by stateful packet inspection.

If there is no external access to the merchant location by Internet, wireless, virtual private network (VPN), dial-in, broadband or publicly accessible machines (such as kiosks), the point-of-sale (POS) environment may be excluded. However, in reality, most POS systems have some form of remote access either from the corporation (frame-relay or VPN), or are managed remotely and are, therefore, within the scope of PCI DSS requirements.

Developers build applications for functionality and frequently do not build security into the requirements.

A Typical PCI Engagement

On average, PCI projects last between 12 and 18 months. They begin with the creation of a data flow diagram to determine which systems contain sensitive PCI data. The second part of the engagement requires a risk and vulnerability assessment to be performed on all system components in the cardholder data environment to determine where vulnerabilities need to be addressed. The initial gap analysis and remediation is the biggest hurdle for companies to overcome.

Scanning is the third key component of the engagement and identifies those systems that are not patched, those that contain known vulnerabilities, and weaknesses resulting from default accounts and blank passwords. While internal and external scans need to be completed on a quarterly basis, only the results from the external scans need to be submitted to PCICo. Merchants and service providers need to be mindful of the fact that a scan is considered valid only if it is conducted by an authorized scanning vendor (ASV).[2]

Likewise, merchants and service providers that require an audit must have the work performed by a QSA,[3] who then creates an RoC to be submitted to the acquiring bank.

If an enterprise is not compliant, it must submit a clear plan detailing how compliance will be achieved. This plan is monitored by the company's QSA and acquirer. It may be possible to use compensating controls[4] to meet a requirement, but the compensating control must be over and above what is already specified and must meet the intent of the DSS requirement. Any compensating control is at the discretion of the QSA and must be agreed to by the acquirer.

A very small percentage of customers is compliant to PCI DSS without any form of remediation. Drawing on the experience of the PCI audit team, most enterprises store credit card data in multiple locations and the information is rarely encrypted. Additionally, information that is now prohibited from being stored, such as Card Verification Value 2 (CVV2) or personal identification numbers (PINs), is often found stored in multiple locations. Investigating all the potential places, such as log files, where this information might be stored, is not easy and is made more difficult by the complex nature of the environment. As a result, enterprises often need to review their data retention policies and re-create backup tapes with the information appropriately secured.

In a large complex network, remediating against default accounts and passwords can cause a huge problem. Creating a compensating control, while appropriately built standards are created and the problem remediated, can put immediate controls in place to reduce risk, while a more secure permanent solution is deployed. An example of this would be enabling Secure Shell (SSH) for remote administration and allowing only the remote administration to occur from a secured terminal.

Application vulnerabilities are one of the top security problems. For example, in one case, an enterprise believed because a password was stored within an executable program that the application was secured. The QSA simply used a UNIX utility called "Strings" to examine the binary code of the program and easily revealed the password.

Developers build applications for functionality and frequently do not build security into the requirements. Security becomes an afterthought. Penetration testing at the application level is crucial to understand what vulnerabilities exist. Careless coding is something that can be reduced through good development practices, but to err is human and, therefore, coding errors will never disappear.

A plethora of database intruder-prevention-style appliances is gaining popularity in the marketplace. These appliances will monitor each transaction, looking for activity that corresponds to an attack, such as SQL injection, and raise alerts. Security policies such as the maximum number of credit cards that should be accessed within a day can be configured on these devices, so that they can alert upon policy violations.

The most common egregious PCI DSS audit failures are:

1. Requirement 3: Protect stored data.
2. Requirement 11: Regularly test security systems and processes.
3. Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters.
4. Requirement 10: Track and monitor all access to network resources and cardholder data.
5. Requirement 8: Assign a unique ID to each person with computer access.
6. Requirement 6: Develop and maintain secure systems and applications.
7. Requirement 12: Maintain a policy that addresses information security.
8. Requirement 9: Restrict physical access to cardholder data.
9. Requirement 4: Encrypt transmission of cardholder data and sensitive information across public networks.
10. Requirement 1: Install and maintain a firewall configuration to protect data.

Ongoing Assessment

PCI requires sustained compliance as verified by each level's validation requirements. It is expected that the standard will change to address emerging threats. Companies will have to adjust to meet these new requirements to remain compliant. By raising the enterprise's information security maturity level, it is possible to reduce the cost of the ongoing annual audits. With the right choice of tools, enterprises can defensibly demonstrate their adherence to a broad spectrum of corporate standards and regulations, including PCI compliance, the US Sarbanes-Oxley Act and Health Insurance Portability and Accountability Act, while increasing overall security, achieving continuous compliance, and lowering the cost and complexity of their IT infrastructure.

An example of using tools to simplify the audit process is using a configuration management tool that provides ready-to-deploy support, such as the Center for Internet Security (CIS)'s configuration templates, which are specifically mentioned within the PCI DSS standard. The auditor can look within the management tool's console to ensure that the machines are compliant with a recognized best practice without using sampling techniques. For a large enterprise, this can represent a considerable savings, where the alternative is a manual sampling of 10-15 percent of the machines and the cost of an audit is US $100-$200 per hour.

Another example of tools simplifying the audit process is using a policy management tool. Requirement 12 of PCI DSS specifies that the enterprise has a policy in place that meets all the security requirements outlined within the DSS. The key is that the policy must meet the requirements, and subrequirements are outlined within the standard. Policy management tools map existing policy back to the PCI DSS requirements, allowing an auditor to see at a glance that the existing enterprise's security policy meets the requirements outlined within the DSS.

Conclusion: The Future of PCI DSS

PCI DSS is by no means perfect, but it does provide useful guidance as to the controls that should be used to protect sensitive data. The standard can be used not only to protect credit card data but all personally identifiable information. In 2008, with the advent of Single Euro Payments Area (SEPA), European countries will start cobranding their bank cards with one or more of the card association logos. This will result in a significantly larger number of merchants and service providers in Europe being classified by PCI DSS as level 1 or 2. There have been corresponding noises about introducing consumer data breach notification laws in the European Union (EU) parliament. On 11 May 2007, the Texas (USA) House of Representatives unanimously passed HB 3222, which mandates that businesses that accept payment cards comply with all PCI DSS requirements, effective 1 January 2009. Other states in the US are introducing bills that cover some of the PCI DSS requirements.

The number of security breaches will no doubt continue to increase, and there will be a corresponding increase in legislation globally to force enterprises to put in security measures to protect personal information. The ability to store information about an individual should be seen as a privilege and not a right. Enterprises that do not protect the information should and will have that privilege removed.

Endnotes

[1] Details of the 200 subrequirements are outlined in the security audit procedures at *https://www.pcisecuritystandards.org/tech/supporting_documents.htm*.

[2] A list of authorized vendors can be found at *https://www.pcisecuritystandards.org/pdfs/asv_report.html*.

[3] A list of qualified assessors can be found at *https://www.pcisecuritystandards.org/pdfs/pci_qsa_list.pdf*.

[4] For a definition of PCI compensating controls, please see *https://www.pcisecuritystandards.org/tech/glossary.htm*

Author's Note

The authors would like to thank Jenna Sindle for her editorial assistance.

Doug Drew, CISSP, PCI QSA
is a senior security consultant at BT INS. Drew has more than 10 years of experience in information security and has taught incident response and forensics at the collegiate level. He has been working with the PCI standard since 2006 and has conducted numerous PCI engagements for BT INS, covering a diverse range of industries. Drew specializes in risk management, regulatory compliance and security program development, serving as a trusted advisor to *Fortune* 500 companies.

Sushila Nair, CISA, CISSP, BS 7799 LA, PCI QSA
is a product manager at BT Counterpane and responsible for compliance products. Nair brings 20 years of experience in computing infrastructure and business security as well as a diverse background, including work in the telecommunications sector, risk analysis, credit card fraud and experience as an expert legal witness. She has worked with the insurance industry in Europe and the US on methods of quantifying risk for e-insurance based on ISO 27001. She was instrumental in creating the first banking group in Malaysia focused on using secondary authentication devices for banking transactions. Nair has worked extensively with customers of BT to develop monitoring solutions that meet the needs of regulatory compliance, including that of PCI DSS.

The Top 10 Compliance Project Challenges and Opportunities

By Tarun (Tony) Chandola, CISA, CISM, CISSP, PCI QSA, PMP

To Be Compliant or Not: The Drivers for Compliance

As the bard may have rephrased, "To be compliant or not to be compliant—that is the question. Whether it is better to risk the penalties and breaches of information and consider them to be within the risk appetite or to embrace seemingly outrageous standards and initiate costly remediation processes."

That was the question.

Not any more.

Compliance has always been driven by regulations and breaches. Proactive measures such as having the victim of a major breach, e.g., TJX, become a key spokesperson for compliance, as part of its settlement deal with the credit card company, have improved awareness of the total cost of breaches.[1] The TJX breach was initially estimated to cost US $41 million, based on an estimate of about US $1 for each credit card record. The total cost of the breach is now estimated to be a minimum of US $1.35 billion.[2] The steep increase in the impact estimate is a result of factoring in other costs such as the price of consultants, security upgrades, attorney fees, liability suits and damage-control marketing.

The high cost of nonconformance (as per some estimates to be almost US $100 for each record) has enabled the shift in the question of compliance from "if" to "when" for executives who were traditionally focused on *tangible* return on security investment (ROSI). The consequent diminishing of executive resistance to compliance projects has, therefore, removed a critical barrier toward initiating the remediation projects.

The objective of this article is solely to contribute to a publicly accessible knowledge base of compliance-related challenges. The following sections describe a number of challenges that an enterprise may still face. The challenges noted in the article, though numbered, are not hierarchical or prioritized, as those aspects are dependent on individual organizational factors.

Challenge No. 1: Simplification of Standards and First-stage Euphoria

Case History 1: First Stage Successful, Second Stage Unclear

The enterprise was very confident about meeting the compliance challenge as it had at its disposal an arsenal of different specialists and gap reports produced by industry experts. However, after the gap report phase, the actual remediation process could not get initiated.

Analysis: All complex and challenging compliance regulations/standards, such as the US Sarbanes-Oxley Act, the US Health Insurance Portability and Accountability Act (HIPAA), and Statement on Auditing Standards (SAS) No. 70, which used to cause frustration in the corporate world by virtue of their mandatory nature and punitive powers, have become reduced to Excel "yes, no, definitely, maybe" checklists. This spreadsheet-based simplification has led to an ease in producing gap reports with deficiencies. The remediation process of the identified gaps, however, has not become correspondingly less complex.

Finding faults was easy; correcting them was tough.

Impact: Finding faults is easy; correcting them is tough. The maturity of spreadsheet methodology to conduct audits and generate gap reports has streamlined the first phase of compliance projects considerably. This first-phase success, however, may induce a false sense of optimism about the complexity of the project as a whole.

Opportunity: The simplified audit lists can be leveraged to provide an enhanced awareness of security controls to the security stakeholders for long-term project benefits.

Resolution: The awareness that a gap report is only the first phase of an extensive engagement will assist the team in better planning of the total life cycle.

Challenge No. 2: Certified Remediation Expert

Case History 2: More Auditors and Fewer Remediation Experts

Through the job market, enterprise Y had access to risk managers, project managers, IT auditors and security specialists, but could not find any remediation experts.

Analysis: There is no widely accepted certified gap remediation expert guideline or certification. The required skill for gap remediation is a combination of skills involving knowledge of audit, governance, risk management, project management, change management and communications.

The remediation owner may have to handle various issues ranging from office politics to coordinating acceptance on the compensatory controls by various stakeholders at all levels.

Resolution: The remediation project resource can be an internal team member with the following skills and abilities:

- Understanding the objective, i.e., steady state of compliance
- Planning business process reengineering
- Organizing stakeholder buy-in

- Project management
- Ability to evaluate business impact analysis and risk management
- Ability of persuasion to get executive sponsors/stakeholders aligned with the changes

Opportunity: The security audit project can be leveraged to develop in-house remediation, governance and compliance professionals. Internal resources are usually more effective in terms of cost and organizational alignment.

Challenge No. 3: The Moving Target and "Live" Factors

Case History 3: The Dynamic Factors; Heisenberg Principle

The IT project manager reported that, since the standards had been updated, the project was being impacted indefinitely. The executives were exposed to information about upcoming standards and were aware that some of the critical business processes were dynamic and partially *ad hoc*. They, therefore, agreed that achieving compliance under such conditions was like trying to hit a moving target.

Impact: This acceptance of changes in the project plan due to perceived shifts in the security horizon and an awareness of live business processes formally opened the door for unplanned changes in the project and scope with significant ramifications.

Analysis: Projects have fallen through the gaps of the following dynamic elements:

1. **Moving target of different standards and their different versions**—Standards, like enterprises, mature in response to the changing risk scenario and new regulations. Canada's Personal Information Protection and Electronic Documents Act (PIPEDA) is one of the latest such examples; it is now mandatory for all enterprises collecting private information.
2. **Live processes**—To initiate the compliance process, the auditor may have to confirm the process *status quo*. The process may keep on changing even as the security specialist is capturing/confirming it. The reason is that the process execution owner may regard the consultant, who is doing the process capture, as an external auditor. The process owner, therefore, will try to change the process *ad hoc* to look better. This is similar to the paradox portrayed by the Heisenberg principle: the process of locating the electron will make the electron bounce and change the actual location, making it impossible to be located with 100 percent certainty. Similarly, an auditor will come across challenges in processes, capturing dynamic or immature *ad hoc* processes.

Impact: The combination of the dynamic factors has often created an insurmountable hurdle toward compliance.

Opportunity: See the forest, not the trees.

Resolution:

- 80 percent of the new version will retain the older framework.
- 80 percent of all standards/regulations (i.e., Sarbanes-Oxley, HIPAA, ISO 17799 and SAS 70) correlate to each other. For example, firewall rules, segregation of duties, physical access and policies are common elements of control.
- Every process should be reviewed with owners at every stage—from the point of view of initiation, planning, execution, control and closing.

Analogy: There is a distinct and common substructure pattern that can be discerned in all the standards and processes. All security standards, by virtue of aiming for the same goal of business resilience, share common controls and recommendations. Similarly, all processes have common stages, as indicated in the project management methodology. (See challenge no. 4.)

Challenge No. 4: Perception of Unique Business Process

Case History 4: No Fit Issue

The enterprise could not relate to any standards. It perceived the key process to be unique and, therefore, without any correlation to standard best business practices.

Analysis: Business processes are at times considered unique by the stakeholders.

Resolution: While there is no clear road map, and every business may justify itself to be considered unique, it is possible to:

- Identify key critical business processes and stages
- Review a unique process from the point of view of initiation, planning, execution, control and closing. All processes can be captured by using a Visio flow chart with common process boxes that show inputs, outputs and results.

Challenge No. 5: Lack of Road Maps for Complex Enterprises

Case History 5: Works for Small Enterprises, Fails at Higher Levels

The enterprise knew that in small, isolated departments, compliance could be achieved by using off-the-shelf solutions. It was at the enterprise level where there was a lack of a cookie-cutter solution. It was difficult for the executives to understand how smaller competitors with lesser resources could achieve the compliance validation faster.

Analysis: Lack of customized road maps for large enterprises makes it challenging to have a uniform approach to compliance. For example, the Payment Card Industry (PCI) Digital Security Standards (DSS) have a good set of recommendations suitable for enterprises with lower volumes in credit card transactions and a method of information acceptance. This makes compliance with the same standards achievable for small and medium enterprises, while making it complex for merchants with larger volumes and more complex modes of information collection. For example, a common challenge is that there is no universally acceptable off-the-shelf product to meet the encryption requirements at higher volumes.

Impact: Achieving compliance for a larger and complex enterprise may be more challenging.

Resolution: While there is no defined road map for larger entities, it is possible to:

- Identify key critical business processes and stages
- Break down the remediation program to smaller work streams—projects under a common coordinated steering committee

Challenge No. 6: Pockets of Internal Resistance to Compliance

Case History 6: Executives Agree, Process Owners Resist

The executive team had done an excellent job of identifying the critical business processes and initiated a corporatewide compliance project. However, the project kept on hitting obstructions due to resistance from the actual process owners.

Analysis: The lowering of resistance for compliance-driven changes had not adequately filtered down to the actual process execution owners.

Resolution: Buy-in of the process execution owner. To decrease the resistance of the process owners, the steering committee had to provide evidence of enterprise-level commitment, through strong communications focused on awareness of benefits and an achievable strategy, to coordinate buy-in of all identified stakeholders.

Challenge No. 7: From Compliance to Stepping Into Unplanned *Terra Incognita*

Case History 7: Going Off on a Tangent

Corporation X has huge profits, ensuring that it is high on the radar for compliance. The executives analyzed the enterprise-level compliance activities required and came to the logical conclusion of treating each of the key processes as an individual project. After trying out external resources, the executives decided to be self-reliant and build their own risk and governance management office by leveraging a management policy of internal development. Within a short span of time, the managers provided negative feedback, citing their inability to study and lead remediation projects as well as handle operational duties. This feedback affected the organizational work efficiency in a negative manner.

Analysis: What had started as a series of well-intentioned logical steps to implement remediation projects, resulted in creating an immature governance, risk and compliance projects office.

Suggested resolution: The final resolution was to blend internal and external resources under steering committee leadership. External consultants holding the Certified Information Systems Auditor (CISA), Certified Information Security Manager (CISM), Certified Information Systems Security Professional (CISSP) or Project Management Professional (PMP) certifications were provided with internal key resources to work as co-owners of the remediation process.

Challenge No. 8: "Everyone Owns, No One Owns" Syndrome

Case History 8: Multiple Owners Equals No Owners

The enterprise client had five different departments carrying out simultaneous analogical roles. IT security was divided among the corporate security, information protection, infrastructure security, audit and compliance, and risk management offices/departments. Multiple ownership of security activities enabled the stakeholders to use semantics and other strategies to avoid being identified as the primary compliance stakeholder. Finally, since the data impacted were credit card records, the primary stakeholder was identified as the banking department. This resulted in all the remediation project exceptions being routed to a sponsor whose primary expertise and domain was not security.

Resolution: Identification of process owners through Responsible, Accountable, Consulted and Informed (RACI) charts and appropriate reaffirmation as required

Opportunity: A clear and logical demarcation of roles and responsibilities is the key opportunity offered by this challenge, with an affirmation at the security committee or steering committee level. The identified owners of the remediation process should be prominent stakeholders with adequate expertise and leverage to coordinate the required changes.

Challenge No. 9: No "Easy Button" Solution

Case History 9: The Temptation of the Wonder-tech Solution

The executives were tempted by the ease of the recommended technological solution to meet the compliance challenge. The sales team of the vendor was very persuasive that their application would make the enterprise compliant.

Background: The technological solution was an application that would be able to cross-map the business processes' activity logs and match them against known exception patterns. The executives were fully confident about the vendor's reputation. The IT team was happy with the upgrades in the infrastructure. The process execution owners had an objection. In their opinion, there was an insufficient collection of activity data—logs to be processed. In other words, buying a solution would have suffered from the "garbage in, garbage out" condition, while leaving the root causes of process maturity levels untouched.

Resolution: Since the technological solution required logs of activities to be reviewed for patterns, it was possible for the project manager to show the application dependencies on data collection, staff training and business process maturity. The application implementation plan was revised to include change management, business impact analysis, business process reengineering, retraining of resources and revision of stakeholder expectations.

Opportunity: Technology, processes and people have to be in alignment to work effectively as a control. A strong focus on any one of these, at the cost of the other elements, exposes the entire control to risks. An application may be secure in itself, but if supported by untrained staff or inadequate processes, it can lead to social engineering risks.

Challenge No. 10: Organizational Culture—The Supreme Buy-in Factor

Case History 10: Theoretically, It Should Have Worked

The remediation plan created by external experts should have worked, but it did not provide satisfactory results.

Analysis: The remediation process affects the critical business processes and, thus, the remediation project is a sensitive process, subject to enhanced budget issues, process ownership clarifications, change management and office politics. All of these and more factors contribute to creating an organizational culture with significant influence on the outcomes of compliance projects.

Resolution: While there is no standard categorization of organizational culture or its impacts, the requirement for buy-in from the actual process owners is of paramount importance. The buy-in strategy will be dependent on the organizational culture. In some enterprises, a clear steering committee communication may be adequate, while in others, there may be a requirement to work at a more granular level. A process execution owner's resistance to the compliance changes may be driven by the added onus of providing audit proof-of-process resilience. Such proof may require the process owner to fill out an extra form or key in more information on a new application.

Opportunity: As the Greeks said, know yourself. From an organizational perspective, this would mean an awareness of the organizational work culture to match the implementation of remediation controls and an identification of all the stakeholders at different levels.

Conclusion and the Hidden Benefit of Compliance

The security compliance and remediation project landscape has changed and matured to a new stage, where the identification of the gaps and remediation is not the primary challenge. The current challenge is to map and align the business processes and culture with the planned remediation changes.

Enterprises must be able to understand the resistance to changes and leverage that knowledge to achieve the buy-in of all stakeholders—executives as well as process execution owners.

A universal compliance project resolution tool and strategy should include solid executive sponsorship and support via strong and visible communications. Such a strategy should facilitate identification and acceptance of all actual owners and stakeholders, enabling their buy-in.

A key, but hidden, benefit of the compliance and security project is organizational self-discovery. A review of the security project life cycle and issues can be leveraged effectively as a self-discovery tool. The compliance gaps and process resilience deficiencies have common factors. Thus, organizational self-discovery via a security compliance project will result in a higher level of visibility and awareness of internal issues. Such awareness can be utilized to achieve the final objective of a more resilient business process and the next level of organizational maturity.

Endnotes

[1] US Securities and Exchange Commission, Full Text of TJX's Settlement Filing, USA, 22 September 2007, *http://storefrontbacktalk.com/story/092207TJXfiling.php*

[2] Kark, Khalid; "Calculating the Cost of a Security Breach," *www.forrester.com/Research/Document/Excerpt/0,7211,42082,00.html*

References

Aberdeen Group, "The Value Proposition of Governance Risk and Compliance," GRC Strategic Agenda, February 2008

Privacy Rights Clearinghouse, "A Chronology of Data Breaches," *www.privacyrights.org/ar/ChronDataBreaches.htm*

Dignan, Larry; "Data Breach Miscalculations: TJX's Customers Aren't Leaving," *http://seekingalpha.com/article/34907-data-breach-miscalculations-tjx-s-customers-aren-t-leaving*

Aon Corp., "Legal Exposures to the MAXX; Insurance for Breaches of Data Privacy and Information Security," 1 December 2007, *www.riskandinsurance.com/userpdfs//AonInsuranceDataSecurity.pdf*

Kugele, Norbert F.; James Placer; "Navigating Some Uncertain Waters in Michigan's New Security Breach Notification Law," *www.goisg.com/CMS/media/52.pdf*

Kerber, Ross; "Analysts: TJX Case May Cost Over $1b," *www.boston.com/business/personalfinance/articles/2007/04/12/analysts_tjx_case_may_cost_over_1b/?page=2*

Author's Note

The author wishes to thank Thom Barrie from Information Systems Security Association, the TELUS GRC Team and Rafael Etges for coordination, guidance and support in the development of this article. The views and the opinions reflected in this article are the author's own and reflect the tendencies noted from a vantage point provided by individual experience.

Tarun (Tony) Chandola, CISA, CISM, CISSP, PCI QSA, PMP has more than 10 years of experience in the world of IT security. He has successfully led and coordinated compliance projects for *Fortune* 500 companies, including banks and telecoms. He is currently employed as a senior security consultant for an enterprise with more than 25,000 employees.

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.

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 company would like to develop an Information Handling Policy. Can you help us to stratify the handling procedures as per the risks involved?

A The whole concept of information handling has assumed more significance because of the various security incidents, and it is essential for companies to have a comprehensive standard for it.

I have tried to produce a standard document, based on the inputs I received from a training programme I attended a few years ago during a conference. The trainer assumed that information is classified into four different types based on sensitivity and, accordingly, controls have been maintained.

The usual caveat applies: the list is not complete and it is only an illustrative example.

Area/Domain	DC—Type I	DC—Type II	DC—Type III	DC—Type IV
Access	None	Access to DC—Type II is to be limited to those personnel who have a 'need to know' the information.	Access to DC—Type III is to be limited to those personnel who have a 'need to know' the information.	Access to DC—Type IV is to be limited to personnel specifically authorised to see and handle individual information assets.
Access Control Records	None	None	None	Access control registers (softcopy or hardcopy, as deemed appropriate) are to be maintained on the creation, receipt, movement and destruction of all DC—Type IV documents.
Labelling	None	Paper documents are to be clearly marked DC—Type II at the top of each page. All other media are to be clearly marked DC—Type II in an appropriate manner.	Paper documents are to be clearly marked DC—Type III at the top of each page. All other media are to be clearly marked DC—Type III in an appropriate manner.	Paper documents are to be clearly marked DC—Type IV, with their unique serial and copy number at the top of each page. All other media are to be clearly marked DC—Type IV, accompanied by their unique serial and copy number.
Handling and Storage—Paper	A clear desk policy is to be applied, whereby documents are put away outside of working hours.	Documents are to be processed and stored within XXXXX and trusted third-party premises only. Documents and displays are to be stored in such a way that they cannot be read/accessed by unauthorised people. Documents are to be locked and stored when not in use.	Documents are to be processed and stored within XXXXX and trusted third-party premises only. Documents and displays are to be stored in such a way that they cannot be read/accessed by unauthorised people. Documents are to be locked in a security container of a type approved by the IT security group, when not in use.	Documents are to be processed and stored within XXXXX and trusted third-party premises only. Documents and displays are to be stored in such a way that they cannot be read/accessed by unauthorised people. Documents are to be locked in a security container of a type approved by the IT security group, when not in use.
Handling and Storage—Nonpaper Media	Process only on XXXXXX-owned or -leased systems.	DC—Type II information is to be processed only on XXXXX-owned or -leased systems that are specifically authorised to process such data in the information security policy. Recording media used on such systems and, if fixed media are used, the system itself, are to be physically secured to the standard approved by the IT security group for DC—Type II paper documents. Direct access to such systems is to be limited to personnel authorised to receive DC—Type II information.	DC—Type III information is to be processed only on XXXXX-owned or -leased systems that are specifically authorised to process such data in the information security policy. Recording media used on such systems and, if fixed media are used, the system itself, are to be physically secured to the standard approved by the IT security group for DC—Type III paper documents. Direct access to such systems is to be limited to personnel authorised to receive DC—Type III information.	DC—Type IV information is to be processed only on XXXXX-owned or -leased systems that are specifically authorised to process such data in the system security policy. Recording media used on such systems and, if fixed media are used, the system itself, are to be physically secured to the standard approved by the security manager for DC—Type IV paper documents. Direct access to such systems is to be positively limited to personnel authorised to receive DC—Type IV information.

Area/Domain	DC—Type I	DC—Type II	DC—Type III	DC—Type IV
Publishing/ Release of Information	Unclassified information may be disclosed to XXXX staff and third-party contractors. Moreover, it may be released outside XXXXX on a discretionary basis.	DC—Type II information is not to be disclosed unless there is a business, contractual, legal or regulatory need. Recipients of such information are to be made aware of both the sensitivity level of the information and the security requirements for its protection. It is to be released only to trusted partners, under an appropriate non-disclosure agreement (NDA).	DC—Type III information is not to be disclosed unless there is a business, contractual, legal or regulatory need. It is to be disclosed only on a strict need-to-know basis and with the prior approval of the originator. Assurance is to be sought from recipients of such information that they are aware of both its sensitivity and the security requirements for its protection, and that they will protect it accordingly. It is to be released to trusted partners under an appropriate NDA.	DC—Type IV information is not to be disclosed unless there is a business, contractual, legal or regulatory need. It is to be disclosed only on a strict need-to-know basis and with the prior approval of the originator. Positive assurance is to be obtained that: • Recipients are either XXXXX staff or a trusted partner's staff authorised to receive such information under an appropriate agreement • Recipients understand the sensitivity of the information and the security requirements for its protection, and will protect it accordingly
Snail Mail/ Courier Transmission	None	Internal and external mail is to be placed in a sealed envelope, annotated as 'DC—Type II' and addressed to the intended recipient by name or appointment. When sent externally, the envelope is not to bear any security marking or other indication relative to the sensitivity of the contents.	Both internal and external mails are to be sealed in a single envelope or other equivalent packaging, addressed as 'personal for' the intended recipient and annotated as 'DC—Type III'. Each joint in the envelope or other packaging is to be covered with clear tape. External mail is to be delivered either by hand of a trusted individual or by a trusted third-party courier service provider.	Internal mail is to be sealed in a single envelope or other equivalent packaging, addressed as 'personal for' the intended recipient and annotated 'DC—Type IV'. Each joint in the envelope or other packaging is to be signed or otherwise endorsed, and all endorsements and joints are to be covered with clear tape. Mail sent externally is to be double-enveloped. The inner envelope is to be prepared as for internal mail, before being placed in an outer envelope, which is not to bear any security marking or other indication of the sensitivity of the contents. The outer envelope is to be addressed to the intended recipient, by name and appointment, and annotated as 'to be opened by addressee only'. A receipt is to be enclosed for the recipient to return. External mail is to be delivered by a trusted third-party courier service provider and the recipient should be obliged to sign for the mail on receipt.
Discussions	None	Discussions on DC—Type II information are not to take place in a public place where conversations can be overheard.	Discussions on DC—Type III information are to take place only where assurance can be gained that there is little risk of the conversation being overheard by unauthorised persons directly.	DC—Type IV discussions are to take place only where assurance can be gained that there is little risk of the conversation being overheard by unauthorised persons directly or by the use of technical eavesdropping or surveillance.
Duplication/ Copying of Information	None	DC—Type II documents are to be copied only by XXXXX staff, trusted third parties and contractors authorised to receive such information. Extra copies are to be destroyed.	The copying/duplicating of DC—Type III documents is to be strictly controlled, authorised by the originator, and performed by XXXX staff or trusted third parties only. Proactive steps are to be taken to find and destroy extra copies. Clear distribution lists and copy numbers are to be used to facilitate effective duplication and distribution control.	The copying/duplicating of DC—Type IV documents is to be strictly controlled, specifically authorised by the originator, and performed by XXXXX staff or trusted third parties only. Proactive steps are to be taken to find and destroy extra, including spoilt, copies. Copy numbers and distribution lists are to be used, and the details of the documents produced and their distribution are to be recorded in the DC—Type IV documents register.

Information Systems Control Journal

CPE Quiz

Quiz #120
Based on Volume 3, 2008—Addressing Business Challenges
Value—1 Hour of CISA/CISM/CGEIT Continuing Professional Education (CPE) Credit

Prepared by A. Rafeq, FCA, CISA, CGEIT, CIA, CCSA

True or False

Harries and Harrison Article

1. Common tipping points can come from two sources: internal and external events. An example of an internal event is the enterprise's inability to absorb the changes delivered by new technologies.

2. Major IT project failures, apart from being costly, could also result in reduced market valuation.

3. Executives being asked to approve investment decisions in cases where they see readily identified business justification to do so could lead to a tipping point.

4. The Val IT framework provides useful guidance on proven processes and practices that enable effective governance of investments involving business strategy and IT.

De Haes, Van Grembergen, Ven and Verelst Article

5. CobiT, as an evaluation framework, is useful in evaluating open source software (OSS) because it supports the same business needs and processes and should meet the same criteria as proprietary software.

6. A key issue in OSS adoption is that decision makers may have certain prejudices against OSS, based on outdated information, and consider OSS to be immature and not suitable for organizational use.

7. Although availability of the source code of OSS is one of the major advantages, many studies have shown that most enterprises never actually make use of the source code.

8. Mapping of CobiT with OSS key issues leads to automatic selection of relevant control objectives.

Daigle and Daigle Article

9. Identifying dormant accounts of nonterminated users is listed as a potential CA opportunity.

10. If no laws are broken or no promulgated rules are violated, this means that the most ethically correct behavior is being exhibited.

11. There is no clear difference between CA and CM and, hence, there is no definite threat to the impairment of independence and objectivity.

12. The best response to the ethical dilemma chosen by Amedisys is having the respective management personnel accept ownership for the scripts shared by the IT auditors.

Ott, MacLeod and Mar Fan Article

13. The approach of data mining is different from computer-assisted auditing techniques, as the current technology enables auditors to automatically extract data on a scheduled basis and analyze these data without the need for queries to be embedded in the program source code.

14. An objective of data mining techniques is to uncover patterns indicating process flow and/or develop predictive patterns in business information.

15. Using development methodologies such as agile software development increases the time frame for developing the necessary queries for data sorting and analysis.

16. Auditors should ascertain which values can be used as predictors of critical predictive values, and this can be achieved only by understanding the business process and all of the data elements.

Anderson Article

17. Effective information security requires a balance among elements on which technology depends, such as organizations, people and processes.

18. A new information security model focused on business, not technology, is needed—one that blends technology with the strategic direction and needs of the enterprise.

19. The information security model must be applicable to a specific industry, geography, regulatory and legal system.

20. A critical component of the new model is the interaction of technology with the rest of the enterprise.

21. ISACA's Security Management Committee recognizes the need for a model that cannot be applied internationally, but can be applied to specific cultures and regulatory environments.

Information Systems Control Journal
CPE Quiz
Based on Volume 3, 2008—Addressing Business Challenges

Quiz #120 Answer Form

(Please print or type)

Name______________________________________

Address____________________________________

____

____

CISA, CISM or CGEIT# ______________________

Quiz #120

True or False

Harries and Harrison Article

1. __________

2. __________

3. __________

4. __________

De Haes, Van Grembergen, Ven and Verelst Article

5. __________

6. __________

7. __________

8. __________

Daigle and Daigle Article

9. __________

10. __________

11. __________

12. __________

Ott, MacLeod and Mar Fan Article

13. __________

14. __________

15. __________

16. __________

Anderson Article

17. __________

18. __________

19. __________

20. __________

21. __________

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 the year's end for CPE credits.

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

international
CONFERENCE

We Cannot Thank You Enough

ISACA would like to thank our sponsors, Program Committee and ISACA for their commitment to the 36th Annual International Conference and Annual Meeting of the Membership. The support of our sponsors and volunteers has helped make the International Conference one of the world's leading conferences for IT governance, control, security, audit and assurance.

International Conference Program Committee Members

Bob Darlington, CISA, Chair
Canadian Pacific Railway

Jeffrey Roth, CGEIT, CISA
RSM McGladrey Inc.

Rafael Eduardo Fabius, CISA
Republica AFAP S.A.

Cheryl Faye Santor, CISA, CISM
Metropolitan Water District of Southern California

Phil Lageschulte
KPMG

Vernon Poole, CGEIT, CISM
Sapphire Technologies Ltd.

Sponsors

Gold Sponsor

CASEWARE
IDEA INC.

Silver Sponsor

TELUS®

Bronze Sponsor

ACL™

ISACA®
Serving IT Governance Professionals

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 ____________________________
MONTH/DAY/YEAR

Name____
FIRST MIDDLE LAST/FAMILY

____
PRINT NAME AS YOU WANT IT TO APPEAR ON MEMBERSHIP CERTIFICATE

Residence address ____
STREET

____
CITY STATE/PROVINCE/COUNTRY POSTAL CODE/ZIP

Residence phone ____________________________ Residence facsimile ____________________________
AREA/COUNTRY CODE AND NUMBER AREA/COUNTRY CODE AND NUMBER

Company name ____

Title ____

Business address ____
STREET

____
CITY STATE/PROVINCE/COUNTRY POSTAL CODE/ZIP

Business phone ____________________________ Business facsimile ____________________________
AREA/COUNTRY CODE AND NUMBER AREA/COUNTRY CODE AND NUMBER

E-mail ____

Send mail to
□ Home
□ Business

Chapter Affiliation
□ Chapter Number *(see reverse)*_______________
or
□ Member at large *(no chapter within 50 miles/80 km)*

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

How did you hear about ISACA?
1 □ Friend/Coworker
2 □ Employer
3 □ Internet Search
4 □ *Information Systems Control Journal*
5 □ Other Publication
6 □ Local Chapter
7 □ Certification Programs
8 □ Direct Mail
9 □ Educational Event

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
2 □ Two years
3 □ Three years
4 □ Four years
5 □ Five years
6 □ Six years or more
7 □ AS
8 □ BS/BA
9 □ MS/MBA/Masters
10 □ PhD
99 □ Other
____

Certifications obtained
(other than CISA, CISM, CGEIT)
1 □ CPA
2 □ CA
3 □ CIA
4 □ CISSP
5 □ CPP
6 □ GIAC
7 □ CFE
99 □ Other __________

Work experience
(check the number of years of information systems related work experience)
1 □ No experience
2 □ 1-3 years
3 □ 4-7 years
4 □ 8-9 years
5 □ 10-13 years
6 □ 14 years or more

Current professional activity *(If not your title, please select the BEST match)*
1 □ CEO, President, Owner, General/Executive Manager
2 □ CAE, General Auditor, Partner, Audit Head/VP/EVP
3 □ CISO/CSO, Security Executive/VP/EVP
4 □ CIO/CTO, Info Systems/Technology Executive/VP/EVP
5 □ CFO, Controller, Treasurer, Finance Executive/VP/EVP
6 □ Chief Compliance/Risk/Privacy Officer, VP/EVP
7 □ IS/IT Audit Director/Manager/Consultant
8 □ Security Director/Manager/Consultant
9 □ IS/IT Director/Manager/Consultant
10 □ Compliance/Risk/Privacy Director/Manager/Consultant
11 □ IS/IT Senior Auditor (External/Internal)
12 □ IS/IT Auditor (External/Internal Staff)
13 □ Non-IS/IT Auditor (External/Internal)
14 □ Security Staff
15 □ IS/IT Staff
16 □ Professor/Teacher
17 □ Student
99 □ Other ____________________________________

Date of Birth ______________________________
MONTH/DAY/YEAR

Payment due

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

† For student membership information please visit *www.isaca.org/student*

* 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
France (Paris)	75	$140
Germany	104	$80

✳Call chapter for information

Chapter Name	Chapter Number	Dues
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
Central Ohio (Columbus)	27	$35
Greater Cincinnati, OH	03	$30

Chapter Name	Chapter Number	Dues
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
Los Angeles, CA	01	$25
Orange County, CA (Anaheim)	79	$30

Chapter Name	Chapter Number	Dues
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 IS/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

Advertisers/Web Sites

ACL	*www.acl.com/ISACAJournal*	4
Allied Search*	*www.alliedsearchinc.com*	63
Caseware Idea Inc.	*www.caseware-idea.com/smartanalyzer*	3
CCH Teammate	*www.CCHGroup.com/ISJ*	Inside Back Cover
Computer Associates	*www.ca.com/solutions/infogov*	24
CSI	*www.CSIAnnual.com*	21
Cyber-Ark	*www.cyber-ark.com/ISACA108*	7
ExamMatrix	*www.ExamMatrix.com/ISJ*	18
Favored Solutions	*www.favoredsolutions.net*	6
KBA	*www.kbagroupllp.com*	31
Lander International LLC*	*www.landerint.com*	26
Market Central/SecureSwitch	www.secureswitch.com/reflect	1
Modulo	*www.modulo.com*	10
Paisley Consulting	*www.paisley.com*	32
Pepperweed	*www.pepperweedprocessmodel.com*	14
Prevelant Networks	*www.prevelant.net/easycompliance.com*	Back Cover
Veridion	*www.veridion.net*	11
WizSoft	*www.wizsoft.com*	13

* Position openings/recruitment listings

Leaders and Supporters

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.

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