VOLUME 5, 2010

ISACA® Journal

Governance, Risk and Compliance

Featured articles:

An Approach Toward Sarbanes-Oxley ITGC Risk Assessment

Seven Ways SMEs Can Benefit From GRC Solutions

A Case for a Process-based Approach to GRC

And more...

ISACA®
Trust in, and value from, information systems

WWW.ISACA.ORG

On-site Training

What you need, where you want it, when you need it.

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

www.isaca.org/onsitetraining-save

ISACA®
Trust in, and value from, information systems

MODULO Risk Manager

Comprehensive solutions from the experienced global leader in GRC management

Benefits of Modulo Risk Manager™:

- Complete visibility into risk, compliance and security posture

- Comprehensive integrated platform that automates the entire GRC management lifecycle

- Flexible and secure architecture delivered as software or SaaS solution utilizing an extensive policy knowledge base of mapped framework and compliance controls for immediate return on investment

Contact us

866 663-5802
Toll Free
www.**modulo**.com

MODULO Solutions for GRC
Governance, Risk and Compliance
25 Years

Volume 5, 2010

ISACA® Journal

Columns

Features

Plus

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

Journal Online

Want more of the practical, peer-reviewed articles you have come to expect from the *Journal*? Additional online-only articles will be available on the first business day of each month in which no *Journal* is released, i.e., February, April, June, August, October and December. These articles will be available exclusively to ISACA® members during 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 2010.

Evolution of Federal Cybersecurity—From Individual Controls to Systems of Control
Jeff Roth, CISA, CGEIT

Fundamentals of IT Governance Based on ISO/IEC 38500
Haris Hamidovic, CIA

Health Care Reform Legislation Survival Guide, Part 2
Christopher P. Buse, CISA, CISSP, CPA, Larry Marks, CISA, CGEIT, CFE, CISSP, PMP, and Steve Sizemore, CISA, CGAP, CIA

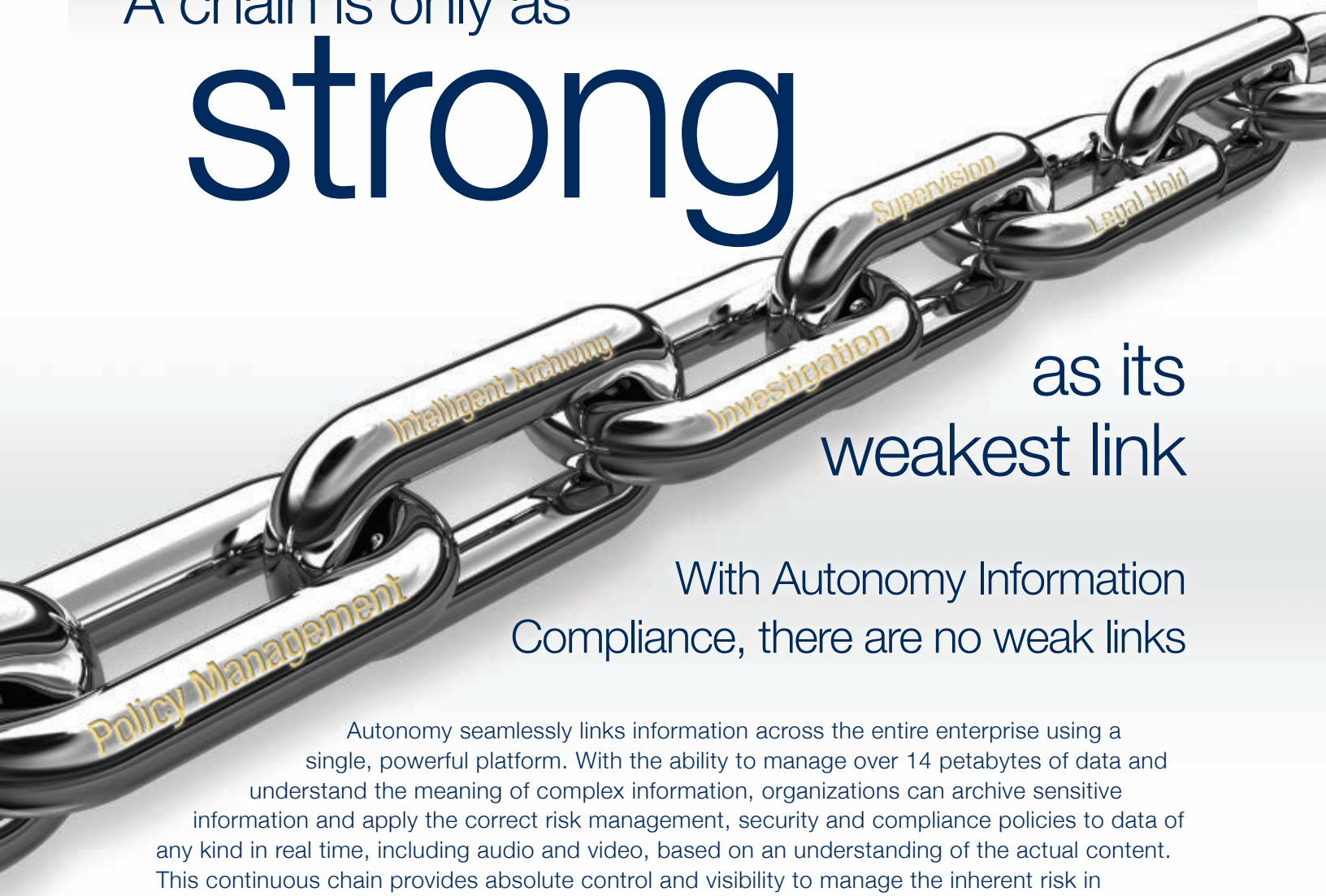
Privacy and Security Considerations for EHR Incentives and Meaningful Use
Stephen Gantz, CGEIT, CEH, CIPP/G, CISSP-ISSAP

Follow ISACA on Twitter: *http://twitter.com/isacanews*

Read more from these *Journal* authors...
Journal authors are now blogging at *www.isaca.org/journal/blog.* Visit the *ISACA Journal* Author Blog to gain more insight from colleagues and to participate in the growing ISACA community.

ISACA®
Trust in, and value from, information systems
3701 Algonquin Road, Suite 1010
Rolling Meadows, Illinois 60008 USA
Telephone +1.847.253.1545
Fax +1.847.253.1443
www.isaca.org

A chain is only as strong as its weakest link



With Autonomy Information Compliance, there are no weak links

Autonomy seamlessly links information across the entire enterprise using a single, powerful platform. With the ability to manage over 14 petabytes of data and understand the meaning of complex information, organizations can archive sensitive information and apply the correct risk management, security and compliance policies to data of any kind in real time, including audio and video, based on an understanding of the actual content. This continuous chain provides absolute control and visibility to manage the inherent risk in business information according to corporate, regulatory and legislative rules.

Leverage the strength of the Autonomy chain:

- 86 of the Fortune 100 use Autonomy Technology
- De Facto Standard for Global Enterprises, Securities Firms, and Regulators
- Only Vendor to Lead in Email Archiving, eDiscovery and Enterprise Search
- World's Largest Private Cloud

Build a chain that works for you—onsite or in the cloud:
www.autonomy.com/compliance

"The fastest growing vendor in the sector."

—IDC, 2009

Autonomy®

The Mayor and the Sheriff

Steven J. Ross, CISA, CISSP, MBCP, is executive principal of Risk Masters Inc. He can be reached at *stross@riskmastersinc.com.*

If information security were a movie, it would be a Western. The chief information security officer (CISO) would be the sheriff, hired to clean up the dusty frontier town—rounding up varmints, corralling rustled strays and protecting the good townspeople from the Dalton Gang[1] (always the Dalton Gang). He would be beloved by the schoolmarm, and he would get along well with the saloonkeeper, too.

This would be a good, interesting movie, especially the climax in which he would singlehandedly shoot down the entire Dalton Gang. There is another story, though, but it is a boring one. It is the tale of the mayor who brought the sheriff to the town. He is really pleased to see crime in check, but he has other worries as well, such as air pollution, unemployment and the building of a sewer system. He has lots of problems to deal with, and on any given day, crime fighting may not be his top priority.

The mayor gets along well with the sheriff and is pleased with the progress he has made, but he does wish the sheriff would stop instigating brawls every night in the saloon and having all his gunfights on the main street.

THE CISO AND THE RISK MANAGER

If the sheriff is the CISO, the mayor is the risk manager.

Historically, information security and risk management have been tightly aligned in most organizations. The lack of adequate protection of information resources has rightly been seen as one of the premier threats to any organization that relies on information systems for its business operations, which, today, means virtually every company and government agency. In recent years, two key factors have put strain on that alliance.

The first, paradoxically, has been the success of information security. When management first comprehended the risks inherent in information technology (often with the prompting of risk management), the result was the appointment of a head of information security, nowadays the CISO, and the allocation of budget to close loopholes, prevent internal misuse of information and protect the organization from the Dalton Gang—er, hackers. There was a perpetual battle for budget, as risks became more evident and effective countermeasures reached the market. So, firewalls, intrusion detection systems, antivirus filters and encryption were introduced, and because they worked, the security of information resources became less risky. Thus, risk managers' attention could be focused elsewhere and CISOs could no longer blithely assume that risk managers would support each of their initiatives and purchases.

In some cases, CISOs' zeal for security exceeds their political skill and the risk manager is an ally in getting senior executives to see things the way the CISO does. The occasional run-ins with management are the equivalent to the Western movie's fistfights in the bar.

The second factor is the emergence of automated information tools in every aspect of business and personal life. The Internet has been around for a while now, but it has never been so pervasive. Significant information processing capability fits in a pocket now, where once it required a briefcase. Many people in many organizations see these devices as tremendous productivity and business growth tools. Many CISOs feel as though they have been through this battle before, when laptop computers became prevalent, and they see the need for improved protective measures. Without arguing the rights or wrongs of each decision, cumulatively these decisions put CISOs on the defensive all the time. They are seen to be against smartphones, against social networking, against flash drives—against, against, against.

Many risk managers take a more measured view of these technical innovations. They can see the potential for both benefit and harm. For the first time in a long while, the CISO and the risk manager are finding themselves on different sides of issues, and both are uneasy with this development.

DIVERGING OBJECTIVES

At the heart of the divergence is the fact that many CISOs are temperamentally inclined and incented to *eliminate risk*, while risk managers are prepared to accept a greater degree of risk for larger rewards, and so they *manage* it. This is more than risk acceptance, which in some places has been code for ignoring risk and hoping that the negative consequences of it never occur (or at

Do you have something to say about this article?

Visit the *Journal* pages of the ISACA web site *(www.isaca.org/journal)*, find the article, and choose the Comments tab to share your thoughts.

least never during the time that the risk acceptor is with the organization).

Even when the risk manager and the CISO agree, there are often differences of emphasis and degree. With a finite budget for security, choices must be made for investment in risk containment. Unfortunately, much of that budget is constrained by the fact that many organizations purchased security products in the past without considering the total cost of ownership (TCO) of those tools. The TCO includes not only annual maintenance fees, but also the continuing labor cost for monitoring and using the safeguards. There is much less to spend in an information security budget than it would seem at first glance. Thus, incremental monies must be spent where the risk is greatest.

Many CISOs are justifiably proud of what they have accomplished to combat misuse of information resources, but are acutely aware that some misuse, some penetration, some data loss may still occur. They are so focused on those continuing battles that they may give less credence than warranted to other risks, such as business interruptions, privacy breaches or system failures, that are caused by errors and omissions, not malicious attacks. It is not so much that they continue to fight the ragged remnants of the Dalton Gang, to continue the metaphor, as it is hard for them to realize that the Daltons do not pose the threat that they used to and that other bad guys have taken over the Dalton Gang's territory. Or, perhaps the town has been pacified enough that some funds can be reasonably released from crime-stopping to pay for some sewers.

All of this is not to minimize the importance of keeping information misuse at bay. There are some organizations, such as banks or the military, in which it is not paranoia to think that there are people in the world out to get them. But, risk can be described as a curve, approaching zero asymptotically though never reaching it. The question that CISOs increasingly must face is whether the curve has inflected to the point at which added investment brings precious little additional security. It is at this point that the mayor's objectives may not be the same as the sheriff's. And, it is at this point that the risks and rewards of the organization need to be considered as a whole, in context.[2]

This does not mean that in all cases the perspective of the risk manager is superior to that of the CISO, but they may be different. And where there are disputes within an organization as to the proper amount or degree of risk that it should accept, risk managers are better positioned to see the issues from all sides. They may, in many cases, but not all, side with the position that more security is needed. If the decision is to accept risk, the CISO has every reason to accept this decision as praise for work well done in the past. This is not a reason to saddle up the noble silver steed and ride off into the sunset.

ENDNOTES

[1] In every good Western, there was always a group of outlaws. There actually was a Dalton Gang that robbed banks in the American West in the 1890s. It seems to me that the Dalton Gang was always the bad guy in the Westerns of my youth.

[2] It is instructive that ISO 27001, *Information technology—Security techniques—Information security management systems—Requirements*, calls for "implementing and operating controls to manage an organization's information security risks in the *context* of the organization's overall business risks" (emphasis added).

CPTRAX

Providing Compliance and Control for your Windows® Enterprise.

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

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

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

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

Use CPTRAX to:

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

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

CPTRAX does not use or require Windows® Event Logs.

Download your FREE EVALUATION today!

www.visualclick.com

Visual Click

Visual Click Software, Inc.
P.O. Box 161657 · Austin, TX 78716
Ph: 512-330-0542 · www.visualclick.com

Mitigating IT Risks for Logical Access

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 articles on fraud, IT/IS, IT auditing and IT governance have appeared in numerous publications, including the *ISACA Journal*.

Unauthorized access can lead to devastating effects. Entities can become victims of malicious activities such as identity theft, financial fraud, theft of data (e.g., credit card data) and attacks on systems (e.g., denial of service), which can be especially harmful for online businesses. All of these harmful effects have been the subject of various news reports in the past.

Criminals, especially IT-savvy ones, have become expert at recognizing weaknesses in access and have become knowledgeable about the tools necessary to successfully exploit weak systems. In fact, experts say more and more criminals are focusing on IT crimes rather than traditional street crimes. Statistics from the Computer Emergency Readiness Team (CERT) and industry security analysts show that about 80 percent of all malicious activities come from current or former employees.[1]

Thus, more than ever, one of the prime concerns in any audit, and for management, is the logical access to computer systems and data. The proliferation of IT, and the Internet in particular, has caused the risks associated with systems and data to explode. In fact, this topic has made the American Institute of Certified Public Accountants (AICPA)'s Top Technology Initiatives every year since 2005 and is ranked first on the 2010 list.[2] Some level of audit risk and business risk exists in virtually every audit because of a variety of IT-related vulnerabilities, but especially access controls.

Earlier this year, this column identified five areas of IT general controls (ITGC) that should be examined in every financial audit.[3] Logical access was one of those five. This article adds further information, in a broader sense of audits, about logical access.

To mitigate the risks associated with access control, it is necessary to identify the risks associated with access controls and to assess the level of those risks. An entity must then establish sound policies and procedures for granting authorized users access while simultaneously protecting itself from unauthorized access. This area of concern is generally considered a subset of identity and access management (IAM). One method for addressing these risks is through the perimeter for authorized access, the process of granting access on only a need-to-know basis (including admin rights) and the process of terminating employees.

MITIGATING LOGICAL ACCESS RISKS

On the perimeter, best practices include authorization and authentication of users in the access rights policies and procedures.

Authorization access controls are those with an objective to ensure that the person seeking access is authorized. This control is most often associated with login credentials and procedures, e.g., requiring an ID and password. However, the hacker world has developed sophisticated tools that can break fairly easily into systems with unsophisticated passwords (names, words found in the dictionary, etc.). Therefore, over the years, best practices have been expanded to include "strong" passwords, frequent changes to passwords and multifactor access controls, as appropriate. The greater the risk, the greater the need for more sophisticated and secure access, and the greater the need for *additional* layers of access controls. The more of the following elements a password includes, the stronger it is considered to be:

- It is at least eight characters long.
- It includes at least one special character.
- It includes at least one number.
- It mixes cases for alpha characters.
- It uses an incoherent phrase (i.e., not an address, etc.).

The purpose of these elements is to thwart existing hacker tools that can guess passwords. Weak passwords and PINs are the major cause for security breaches, according to IT consulting firm Frost & Sullivan.[4] Usernames and passwords/PINs are usually static or shared across multiple accounts by users, making them

relatively easy prey to hackers and crackers. The security profession and financial institutions have responded with temporary PINs and other tools and procedures.

Authentication controls have a different objective. They attempt to ensure that persons logging in to the system are who they say they are. One classic illustration of this extra layer is biometrics. That is, controls are not sufficient where risks are relatively high and the access controls consist of only an authorization control with one layer—ID and password.

> "Controls are not sufficient where risks are relatively high and the access controls consist of only an…ID and password."

Most savvy IT managers add tools such as USB tokens, smart cards, temporary PINS and biometrics on top of ID and password. A USB token, such as one from Entrust or Aladdin, is a hardware device that must be connected to the remote computer in a USB slot before access will be granted. Smart cards are swiped on a reader—similar to the way credit cards are used—on the computer and are combined with the ID and password to grant access. Temporary PINs are numbers sent back to a prearranged device, such as a text message to a cell phone or a small pager device, in which, to gain remote access, users have a limited time to enter the PIN along with their ID and password. The greater the risk, such as a remote login to sensitive data, the greater the need for strong controls for authentication.

However, it is not enough to protect the perimeter. According to CERT in a white paper titled "An Introduction to Insider Threat Management," over the last 10 to 15 years, organizations have spent billions of dollars building stronger defenses to protect their data and systems from hackers and external malicious parties. On average, more than 75 percent of corporate IT security budgets is directed toward protecting against outsiders, even though the annual Computer Security Institute/FBI Computer Crime and Security Study continues to show that insiders were responsible for just as many incidents as outsiders. A 2009 *Information Security Magazine* survey shows the biggest increase in IT spending is in the area of IAM, with the biggest driver being preventing unauthorized access of sensitive information by employees.

Once logged in, even an authorized user should be constrained from having access to all data and applications. Employees should have access to only those applications necessary to do their particular job. That limitation also includes data access rights of read-only, read/write or no access, where applicable (i.e., need-to-know access). For instance, a good security policy would be to have a strong logical access system on the network to log in to the system (e.g., Active Directory applied effectively on Microsoft SQL Server). But then, where risks are high, the entity should have another system of login credentials and access granted for each key application. Some application systems, such as Microsoft Dynamics, provide their own access control as a separate layer of security over data access via the applications. If both of these access control systems are managed properly, someone's ability to break through the perimeter can be mitigated by strong access controls in the "back office" system—that is, a strong pair of controls to prevent unauthorized access. This need-to-know approach to applications is a key element of sound access controls.

Administrative access rights are a critical area that need controls because of the broad access rights "admin" has once logged into the system, and they are included as part of "need to know." Adequate access controls should provide for the application of best practices for the administrator function of databases or database management systems (DBMS), such as DB2, Oracle and SQL Server. They include, but are not limited to, not using a default ID/password for admin, minimizing the number of employees with admin access and establishing some modicum of segregation of duties. Admin rights are especially critical for operating systems in which root access can be granted, giving someone "the keys to the kingdom." Obviously, this area is another that should be examined during most IT audits of any nature.

Lastly, when employees are terminated, there should be effective controls in place to terminate the employee's access to the systems. At termination, entities sometimes forget about logins and access rights formally granted to employees. All entities need an effective control or set of controls to ensure that all terminated employees lose all access rights.

An effective and logical approach is to tie access control to human resources (HR) procedures. When an employee is hired, transferred or leaves the organization, the HR procedures should include the requisite changes to that employee's access rights. When a new employee is hired, that person's "need to know" should be assessed and access rights should be granted to only those applications and data necessary for that person's job responsibilities. Either the

application or the network software should have the means to limit access appropriately. If an employee is transferred, those access rights may change because of the different responsibilities involved in the transfer. Thus, the HR transfer process should include a review of and a change, if necessary, in access rights. When an employee leaves the organization for any reason, but especially if the employee is fired, access rights should be terminated as close to the person's termination as possible, but no later than the person's last day on the job.

CONCLUSION

The IT auditor should consider the previously disclosed procedures in an audit to ensure that access controls are adequate to mitigate the risks associated with access, including limiting the access of legitimate employees to need to know, and mitigating the risk of an unauthorized intrusion.

ENDNOTES

[1] Hirschhorn, Karen; "Hacker Activities," *IT Defense Magazine*, December/January 2007, p. 12-15. See also the Insider Threat Research web page at *www.cert.org/insider_threat/*.

[2] Per the 2010 AICPA Top Technology Initiatives Survey conducted mid-2010. Question: "Which top ten technology considerations are driving your business or practice today?" Number one answer: "Security of data, code and communications/data security and document retention/ security threats." See *http://infotech.aicpa.org.*

[3] Singleton, Tommie; "The Minimum IT Controls to Assess in a Financial Audit (Part II)," *ISACA Journal*, vol. 2, 2010

[4] Ayoub, Robert; "An Overview and Competitive Analysis of the One Time Password (OTP) Market" (White Paper), Frost & Sullivan, June 2009, *http://whitepapers.techrepublic.com.com/abstract.aspx?docid=1016477*

YOUR

SUPPORT

TEAM'S

SILVER BULLET.

QUICK ON THE DRAW

AND

QUICK TO SOLVE!

A legendary support team is already in your office — they just need the right tool. GoToAssist connects your team with your customers like never before with simple, powerful remote support.

GoToAssist® EXPRESS™

by CITRIX®

Try It FREE for 30 Days

www.gotoassist.com/isaca

Robert Schperberg, CISM, EnCEP

Robert Schperberg is Chevron's global IT forensics investigations lead. Previously, he was worldwide director of incident response and digital forensics for Global Integrity, a subsidiary of the Science Applications International Corporation (SAIC). Some of his assignments included conducting high-tech forensics training for the US Federal Bureau of Investigation (FBI) National Information Protection Center's team of the National Security Agency (NSA) and high-risk and high-tech incident response training for MCI and the Denver Downtown Business Association during the Oklahoma City (Oklahoma, USA) bombing federal trial.

Schperberg was also selected through the Defense Information System Agency (DISA) to conduct high-tech and digital forensics investigations training for some of the top US military bases, including Strategic Command (STRATCOM), Central Command (CENTCOM), Special Operations Command (SOCOM) and Transportation Command (TRANSCOM). He was used in an advisory capacity by the French authorities regarding the 11 March 2004 Madrid train explosion investigation, and he has served as a lead digital forensics investigator and advisor in major national and international investigations. Schperberg is also a certified expert witness and has served as such in several high-profile cases.

Schperberg is a retired law enforcement officer from Northern California (USA) and has received multiple commendations and a Computer Forensics Officer of the Year award for his service. He is the author of *Cybercrime: Incident Response & Digital Forensics*.

Q What do you see as the biggest security threats/risks? How can businesses and individuals protect themselves?

A In the economic downsizing that organizations are faced with today, insider threat ranks highest and is of the highest concern for the corporate IT and corporate investigative divisions. Those who are inside the security perimeter and are about to be let go due to the reduction in force have access to intellectual properties, research and development documentation, and ongoing business deals that could seriously affect the organization's bottom line.

Another facet of the downsizing threat is the motivation to exact revenge on the organization. With the availability of malware technology throughout the web, the people who want to commit an act of sabotage do not have to be very technical and can purchase the technology to suit their deed. Additionally, with the advance of technology comes the creation of malware, Trojans, spyware, worms and viruses, which rank a close second. Antivirus companies are struggling to produce antidotes for Day 0 and Day 1 viruses.

Next on the list are the phishing and spear phishing attempts on unsuspecting Internet users and company executives. Phishing is the impersonation of the organization through e-mail or other electronic means in an attempt to obtain confidential information; spear phishing is the targeting of executives by convincing them to click on a link that will download malware or Trojans on their computers.

Last among the top security concerns are fraudulent transactions that result in financial loss or damage to the organization's reputation or its customers.

All sectors, private and public, have to be prepared when downsizing personnel. That entails limiting access to outgoing personnel while generating countermeasures in the event that a malicious attack is being contemplated. That requires the review of all compliance rules and additional training to the computer emergency response team (CERT). For external attacks, such as phishing and spear phishing, continuous training and education of executives and nontechnical personnel is a must. Finally, having proactive measures established in the areas of monitoring and alerts will ward off the number of attacks, while the alerts will enable the CERT to respond at a much quicker pace.

Do you have something to say about this article?

Visit the *Journal* pages of the ISACA web site *(www.isaca.org/journal)*, find the article, and choose the Comments tab to share your thoughts.

Q **Please describe your transition from law enforcement, in the early part of your career, to your current role in corporate computer forensics. What led to this transition, and how has your background supported your current career?**

A While in law enforcement, I became an expert in crime scenes and digital forensics investigations. I was also fortunate to receive several specialized certifications in the area of investigations—homicide, robbery, sexual assaults, computer investigations and fraud/embezzlement. When I was injured on duty and subsequently underwent back surgery, the medical decision was for me to retire. I used a sum of money allocated for rehabilitation to go through technical certification classes offered by Microsoft, Guidance Software and Access Data.

My first job in the corporate environment was with MCI as a senior investigator for corporate security. As such, I conducted several investigations involving threats, fraud and digital forensics. One of the investigations I participated in was that of the Oklahoma City bombing. I moved on to work for other consulting companies including SAIC. Throughout my experiences, I got involved in major, high-profile investigations, gaining experience through each investigation. I was also constantly attending technical workshops in the areas of IT and digital forensics to keep up with technology. Among the highlights were conducting training to some of the top military bases in the US and becoming a certified expert witness. My experiences and continued education paid off when I was offered a position as the global IT forensics investigations lead with Chevron.

Q **How do you believe the certifications you have attained have advanced or enhanced your career? What certifications do you look for when hiring new members of your team?**

A Throughout my career, I obtained several investigative certifications, which included state of California certifications, and US federal certifications from the US Department of Justice (DoJ), the FBI and the US Secret Service. When I transitioned to the private sector, I obtained some Microsoft certifications as well as the Certified Information Security Manager (CISM) from ISACA.

The general trend when searching for cybercrime investigators or digital forensics investigators is to find candidates who have expertise in one of the following fields: digital forensics software and tools knowledge or network and operating systems knowledge. In essence, one candidate or the other will have certifications in their specific field. In today's environment, however, what is needed are candidates who have the technical knowledge and investigative and digital forensics knowledge.

Q **How do you think the role of the security professional is changing? What would you recommend to security students or new security professionals to better prepare them for this changing environment?**

A The security professional's role has constantly evolved around the general practitioner and the specialized practitioner. To those starting in the field of IT or IT security, my recommendation is that they learn as much as possible while gaining as much experience as possible. Setting five-year goals can help to keep candidates focused on reaching goals while improving their knowledge and enhancing their skills. My advice is to transfer to different IT departments to gain different knowledge. Once a candidate is comfortable with the environment, the specialization process should be started. Most companies in a down economy will turn their attention to the experts first then to the "jack of all trades" next, so being prepared will help one maintain or find a position quicker.

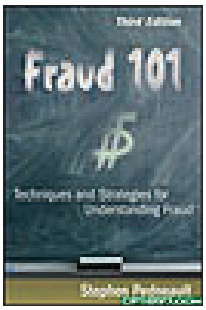
Q **What has been your biggest workplace challenge, and how did you face it?**

A After retiring from law enforcement and having had all that experience and investigative expertise, I had to adjust to the private sector and corporate environment. It was time to earn the employer's confidence by producing results while reinforcing the earned certifications.

Pressure in the private sector and corporate environment is also different. Employers want to see maximum results with minimum expense. The security environment is a necessity, but it does not produce revenue; it does, however, have a cost to the bottom line.

From the technical perspective, I encountered my biggest technical challenge during the Code Red virus/worm time. I had to deploy all my teams, myself included, around the world without any time off to eradicate the infestation from our client's network environment.

Fraud 101: Techniques and Strategies for Understanding Fraud, 3rd Edition



By Stephen Pedneault, CPA, CFF, CFE

Reviewed by Gail Michaelson, CISA, PMP, SSGB, an IT professional from Cincinnati, Ohio, USA, with more than 10 years of expertise in business process optimization and continuous improvement, program and project management, portfolio management, strategic planning, budgeting, and IT auditing. Her industry exposure spans health care, pharmacy benefits management, financial and government services, large retail, education, telecommunications, logistics, and manufacturing. Michaelson is a member of the ISACA Publications Subcommittee.

Do you have something to say about this article?

Visit the *Journal* pages of the ISACA web site *(www.isaca.org/journal)*, find the article, and choose the Comments tab to share your thoughts.

Fraud 101: Techniques and Strategies for Understanding Fraud, 3rd Edition is a primer on how fraud works and how to prevent, detect and prosecute it. The author, Stephen Pedneault, explains fraud in a practical, easy-to-understand manner, introducing general business professionals and nonaccountants to this specialized field. Its intended audience is those with little knowledge or hands-on experience preventing, detecting or investigating fraud. Throughout the book, Pedneault provides solid evidence that fraud is a genuine issue, impacting every organization and social program in operation.

The first half of the book is devoted to providing an overall working foundation for the topic of fraud. Topics reviewed include how great the fraud problem has become, estimated fraud losses and costs associated with fraud plots, and some financial areas commonly abused by fraud.

Although fraud has become a burgeoning industry, only the most heinous cases receive media and legislative attention, such as Bernard Madoff's Ponzi plot and the underhanded plots exposed underlying the subprime mortgage-lending industry. Pedneault goes beyond the headlines to make it clear that fraud can and does occur in all organizations, in both for-profit and nonprofit organizations, and that all industries are at risk from fraud.

Major types of fraud are reviewed. Pedneault points out that fraud is not limited to white-collar crime, such as financial disclosures and reports issued to investors and lenders. Fraud also includes political malfeasance and embezzlement, and individuals invent new plots daily. Some high-level insight into why fraud occurs is offered.

The second half of the book explores the accounting and financial industry's response to fraud, as new fraud plots are identified. Responses to fraud reviewed include US Sarbanes-Oxley legislation, the development of audit committees, the establishment of codes of ethics, internal controls and internal audits, the creation of the Public Company Accounting Oversight Board (PCAOB), new professional credentials, training, and other industry responses.

Defenses against fraud are covered next, with the primary defense being an organization's system of internal controls, followed by education to address the increasing frequency of fraud. Pedneault provides details of different underhanded plots commonly perpetrated, plus warning signs and symptoms of each underhanded plot to increase the probability that detection will occur. Also included are recommended steps and measures an organization should take to investigate known or suspected instances of fraud.

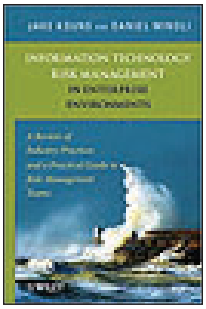
The strength of the 234-page book is that it is both comprehensive and straightforward, providing examples of fraud plots that can be easily understood by those with different levels of accounting knowledge and experience. General concepts are enhanced with real-world case studies that illustrate the fraud issues and cases reviewed. Each case study includes realistic advice on how the fraudulent activity could have been prevented or detected earlier, thereby minimizing the financial loss experienced by each organization.

Fraud 101: Techniques and Strategies for Understanding Fraud, 3rd Edition builds on the previous editions of *Fraud 101* by Howard David and Howard Silverson and is a practical reference guide for all IT and business managers. It should be a useful desktop reference for beginning readers across all industries and geographical areas.

EDITOR'S NOTE

Fraud 101: Techniques and Strategies for Understanding Fraud, 3rd Edition is available from the ISACA Bookstore. For information, see the ISACA Bookstore Supplement in this *Journal*, visit *www.isaca.org/bookstore*, e-mail *bookstore@isaca.org* or telephone +1.847.660.5650.

Information Technology Risk Management in Enterprise Environments



By Jake Kouns and Daniel Minoli

Reviewed by Vishnu Kanhere, Ph.D., CISA, CISM, AICWA, CFE, FCA, an expert in software valuation, IS security and IS audit. A renowned faculty member at several management institutes, government academies and corporate training programs, Kanhere is a member of the Sectional Committee LITD 17 on Information Security and Biometrics of the Bureau of Indian Standards. He can be contacted at *vkanhere@vsnl.com* or *vishnukanhere@yahoo.com*.

Information Technology Risk Management in Enterprise Environments provides an overview of industry practices and a practical guide to IT risk management frameworks, methodologies and techniques. The proliferation of cyberattacks; compromises of IT systems; and the increasing incidence of security breaches in volume, size, value and number have been a cause of concern in corporate and government circles alike. Business, industry and even nations are alarmed at the systematic attacks of ever-increasing magnitude, scale and frequency. Risk assessment and risk management have acquired an important place in the corporate environment as well as enterprise management and governance framework. A quantitative evaluation of potential vulnerabilities, and the consequences and impact of their exploitation by threats that materialize, has become essential for survival. Post-risk-assessment risk mitigation methodologies have become synonymous with good governance over IT.

Information Technology Risk Management in Enterprise Environments is not industry-specific. It addresses all sectors of business, industry and even public/government sectors because risk, by its nature, and IT risk, due to the use of IT in all organizations, are all-pervasive. The book refers to US and European legislation and standards, but it is nevertheless applicable to all geographic areas.

> "Risk, by its nature, and IT risk, due to the use of IT in all organizations, are all-pervasive."

The book is comprised of two parts of five chapters each: Part I covers industry practices; Part II provides guidance to develop a risk management program. The material is well organized with appropriate figures and tables. The book also has a useful glossary and an index for ease of reference. One of its strengths is that it provides 10 appendices, a reference section for each of the 10 chapters and a glossary, providing appropriate documentation for the reader. It could have added further value if the text were embellished by interactive case studies.

The book provides a management perspective and a practical approach to implementing a risk assessment and a risk mitigation process using a team approach. It provides a survey of industry practices, and it is a good guide for developing a framework for IT risk assessment and mitigation in the enterprise.

One of the highlights of the book is that it deals with IT risk management methodologies such as COBIT and Octave. COBIT is widely referenced, and the methodology is explained in detail.

Overall, *Information Technology Risk Management in Enterprise Environments* is a useful book for information security managers, security analysts, systems developers, auditors and consultants, and it even would be of help to academics and students. It is a how-to/reference book, as well as a useful addition to the business library.

EDITOR'S NOTE

Information Technology Risk Management in Enterprise Environments 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.

An Approach Toward Sarbanes-Oxley ITGC Risk Assessment

Arvind Mehta, CISA, C-EH, ISO 27001 LA, manages a global IT Sarbanes-Oxley program for the Technology Risk Services practice at EXL Risk & Financial Management, a *Fortune* 1000 company. His responsibilities include managing IT risk advisory projects with a focus on enterprise risk management, IT security, Sarbanes-Oxley section 404, Payment Card Industry (PCI) reviews, IT infrastructure reviews, vulnerability assessments, application security assessments, enterprise resource planning (ERP) security and separation of duties (SoD) reviews for PeopleSoft. Mehta has in-depth knowledge and understanding of enterprise risk management; IT security; and governance, risk and compliance (GRC) domains. With more than eight years of experience, he has worked with industry leaders in the food and beverage, staffing, insurance and banking, and health care industries.

Do you have something to say about this article?

Visit the *Journal* pages of the ISACA web site *(www.isaca.org/journal)*, find the article, and choose the Comments tab to share your thoughts.

The US Sarbanes-Oxley Act is an old bandwagon for most of the publicly listed companies, as they have been riding on it since its inception in 2002. But, most companies face newer challenges every day with the birth of newer technology, rapidly changing business conditions, and/or mergers and acquisitions.

Even after eight years of Sarbanes-Oxley, companies are still struggling to identify the right scope and the appropriate approach toward Sarbanes-Oxley IT general controls (ITGC). Lack of knowledge to identify the right scope can lead to an increase in the overall cost of compliance since organizations may test applications that would otherwise be deemed out of scope if an appropriate risk assessment had been performed.

The question that should be asked is, what should companies do to identify the exact scope for ITGC? Not only is it important to identify the systems that would fall into the scope of Sarbanes-Oxley, it is also important to identify the extent to which a specific system should be tested. For example, an auditor would definitely perform detailed testing for the financial system of records (SAP or PeopleSoft), but would not spend too much time or cost on performing the same level of testing for a system that falls into the scope but has only a handful of system administrators managing it.

> "What should companies do to identify the exact scope for ITGC?"

The most appropriate and effective way to define the right scope and the extent of testing for each Sarbanes-Oxley in-scope system is to perform a risk assessment focusing on the risks associated with Sarbanes-Oxley requirements and specific to ITGC. Risk assessment is not a new buzzword—everyone in today's world talks about risk-based approach, risk assessments, etc., but few understand that for a risk assessment exercise to be successful, it is extremely important to identify whether the focus of risk assessment is confidentiality, integrity and/or availability, and then to define the risk criteria/parameters.

For example, a risk assessment exercise for Payment Card Industry (PCI) Data Security Standard (DSS) compliance focuses on what should and should not be stored to ensure that credit card information is not compromised and, thus, to ensure data privacy. However, for Sarbanes-Oxley, the same approach cannot be applied because Sarbanes-Oxley focuses on data integrity and misstatements to financial reporting. Therefore, the risk assessment criterion shifts from data privacy to data integrity.

The right approach to identify the exact scope and extent of testing for Sarbanes-Oxley ITGC is to perform a detailed risk assessment that is focused on the risks that are associated with each general control process area, such as change management, logical access, computer operations, job scheduling, and third parties/service organizations that manage applications or data centers.

IDENTIFY RISK CRITERIA/PARAMETERS

The organization's approach to Sarbanes-Oxley risk assessment should identify the key risk parameters that would help to quantify the risks for ITGC. An application might be considered "high risk" when viewed from a change management perspective because it might undergo hundreds of changes every month, but it might be "low risk" when viewed from a logical access perspective because it has only four to five administrators and no end users accessing the application.

To identify the appropriate risk parameters to perform a risk assessment for Sarbanes-Oxley ITGC, the focus should be on integrity and access risks.

INTEGRITY RISK

Integrity risk encompasses all of the risks associated with the authorization, completeness and accuracy of transactions as they are entered into, processed by, summarized by and reported on by the various application systems deployed by the organization. These risks pervasively apply to every aspect of an application system that is used to support the core financial system.

The following are the critical parameters that could impact the integrity of a financial application:

1. **Number of changes**—The number of changes made to a financial application is directly proportional to the risk—the more changes, the higher the risk.
2. **Number of application controls**—If an application is completely automated and the output produced is relied upon for financial reporting without manual intervention, it becomes critical to ensure that all automated application controls are effective. Again, the more automated the application controls, the more reliance on the application and the higher the risk.
3. **Developed in-house**—This parameter is critical to identify appropriate risk levels. If an application is homegrown and an internal team of developers has access to modify and maintain the application, the associated risk should be high; whereas, if an application is commercial, any changes to the source code will need vendor intervention and appropriate methods.
4. **Number of developers**—The number of developers is again directly proportionate to the risk associated with inappropriate application configuration and is a critical parameter in evaluating risk levels.

ACCESS RISK

Access risk focuses on the risk associated with inappropriate access to financial systems, data or information. It encompasses the risks associated with improper segregation of duties, the integrity of financial data and databases, and information confidentiality.

The following are the critical parameters that could impact access to a financial application:

1. **Number of users**—The number of users accessing the application has a direct impact on the risk of unauthorized access and unapproved transactions—the more users, the more risk. An application with three users would probably be considered to have low risk; however, an application with 30,000 users will have a higher level of risk because there will be more chances of human error while granting access, of granting conflicting access or of inappropriate access monitoring.
2. **Number of administrators**—Similar to the number of users, the number of administrators managing the application has a direct, proportionate impact on risk levels.
3. **Direct access to the underlying database**—This is a critical parameter, as it can leave backdoor entries for users with direct access to the underlying database. Few applications store user information within the application, and direct access to the database is not allowed; whereas, some applications allow users to directly access the database without going through the application. Again, the risk will be high in the latter case.
4. **Integrated/independent authentication**—It is very important to evaluate the authentication mechanisms in place for a financial application to determine the list of people who have access to the application. If an application uses integrated authentication with the operating system, the risk is high because users who are approved to manage the operating system would also be granted access to the application; whereas, if the application has its own authentication mechanisms, the risk will be low because even though a person might be an administrator of the operating system, he/she would require an application ID to access the financial application.

The above identified risk parameters can help determine/quantify the actual risk levels for each financial application from an ITGC perspective. A risk scale of low, medium or high is used in the following example, as a demonstration, to calculate the risk ratings for the applications. The risk scale for Sarbanes-Oxley can be defined as shown in **figure 1**.

IMPLEMENTATION OF RISK ASSESSMENT

The following example demonstrates the implementation of the risk assessment approach.

Company ABC Inc. has two financially critical applications used for financial reporting purposes (see **figure 2**). App 1 is the financial system of records and is a commercial application that can be customized, but no development is possible. Any development effort requires contacting the vendor. App 1 has about 150 end users from the accounts payable (AP), accounts receivable (AR), general ledger (GL) and payroll departments, who enter financial data. The

Figure 1—Risk Definitions for Sarbanes-Oxley		
High Risk	**Medium Risk**	**Low Risk**
1. Potential significant impact to revenue or earnings 2. Material to the financial statements 3. Could result in external audit qualification 4. Could result in significant fines or legal action—serious failure to comply 5. Potential significant business interruption 6. Should be communicated to the board of directors if it occurs	1. Potential moderate impact to revenue or earnings 2. Potentially material to the financial statements 3. Could result in management letter from external audit firm (significant issues) 4. Failure to comply with legal or regulatory requirements in some instances 5. Potential business interruption 6. Should be communicated to executive management if it occurs	1. Slight to no impact to revenue or earnings 2. Not material to the financial statements 3. No major external audit findings or issues 4. Failure to comply with legal or regulatory requirements in nonserious and isolated cases 5. Minimal business interruption 6. May need to be communicated to functional leader if it occurs

application has a Structured Query Language (SQL) database that is maintained by two administrators, and no end users have direct access to the database due to security designed within the application. App 1 has its own authentication mechanism. Since App 1 is a commercial application, not many changes are performed, but historical data show that about two changes are performed annually. Since this is a commercial application, the vendor has built several application controls (approximately 25) that control the environment to produce accurate financial reports and results.

App 2 is a homegrown application and is maintained by 20 developers, and about 100 end users access it. It has a database that is maintained by 10 system administrators. The database can be directly accessed by the users if they open an Open Database Connectivity (ODBC) connection outside of the application. The application has integrated authentication with the underlying Windows operating systems. Since it was developed in house, the number of changes is on the higher side—close to 300 annually, according to historical data. No application controls are built into this homegrown application.

The results of risk assessment for these two applications show that App 2 is rated a high risk from a Sarbanes-Oxley ITGC perspective and needs controls to be established to gain reasonable assurance about the integrity of financial data. Since the number of changes made to the application is high, an auditor should test all aspects of change management, including predevelopment approvals, testing (unit, stress and integration, as applicable), verification of test plans and test results, quality assurance testing, separation of environments (development, test, quality assurance, training, production), segregation of duties (no developer access to production), premigration approval, verification that migration is done by authorized individuals, and postimplementation control to ensure that the change is working as expected and that nothing "broke." Similarly, for logical access, both prevent and detect controls (such as user provisioning/deprovisioning, monitoring of security logs, user access reviews and appropriate password controls) should be established.

App 1 is rated as low risk due to the lower number of changes made to the application and lack of development effort being done internally. For a low-risk application, the organization can consider testing only critical preventive controls, instead of doing a full-blown ITGC testing. For example, for change management, only a preproduction approval should be sufficient, since all development and testing is performed by the external vendor, and all other change management controls can be referred to a Statement on Auditing Standards No. 70 (SAS 70) report or an equivalent. Similarly, for logical access, controls such as system administrator reviews can be eliminated because there are only two administrators and direct access to the database is not allowed. For low-risk applications, preventive controls such as appropriate password configurations and provisioning/deprovisioning provide enough assurance that the applications are secure and the necessity of detect controls can be eliminated using this approach, which will result in fewer controls and reduction in overall cost of compliance.

Once an organization has identified the high-risk and low-risk applications and the controls are established and tested for appropriateness, the internal audit department should analyze the trend for failures and effective controls to evaluate whether more controls should be implemented for certain applications and whether some controls can be eliminated for others. For example, if changes to password configuration controls are very rare and have been effective for a period of

Figure 2—Risk Assessment of Financially Critical Applications at Company ABC					
Integrity Risk					
Application Name	**Number of Annual Changes**	**Number of Application Controls**	**In-house Development**	**Number of Developers**	**Risk Level**
App 1	2	25	No	0	Low
App 2	300	0	Yes	20	High
Access Risk					
Application Name	**Number of End Users**	**Number of Administrators**	**Direct Access to Database**	**Authentication**	**Risk Level**
App 1	150	2	No	Independent	Low
App 2	100	10	Yes	Integrated	High

time, the control can be put on rotation, where it is tested every two years to reduce the overall effort of testing and cost as well to reduce the load on the IT department. Similarly, if changes are rare for an application (as was the case with App 1 in the previous example), those controls can be performed by inquiry, instead of a full-blown test, to confirm if any changes were made to the application, and further testing can be done only if changes were made. If the trend analysis shows that the controls are effective year on year and, most important, if there is no feedback or issues raised by the external auditor, existing controls are clear enough to ensure that all financial transactions are secure and reliable.

CONCLUSION

Using this approach, focusing on the parameters that are critical from the Sarbanes-Oxley ITGC perspective, internal audit departments across the organizations can save a lot of time, effort and money and also reduce the load on the IT department. Performing risk assessments periodically with the right parameters in place can be used by audit management as a basis to gain comfort that all systems are being validated and tested as required by the Sarbanes-Oxley ITGC requirements. This will reduce the probability of any significant deficiencies and increase external auditors' confidence in management's testing. If the scope of the ITGC audit is appropriate, the extent of manual procedures that an external auditor will typically perform will be reduced, which will further reduce the overall cost of compliance.

> "Focusing on the parameters that are critical from the Sarbanes-Oxley ITGC perspective…can save a lot of time, effort and money and also reduce the load on the IT department."

EDITOR'S NOTE

Collaborate with ISACA members and access additional resources on this topic in the ISACA Knowledge Center located at *www.isaca.org/knowledgecenter*.

The best stories have a happy ending...

Chapter I - Data Warehouse Software

Once upon a time... Our audit data was stored in different documents that didn't talk to each other.

But now... Audit Leverage gives us a single data warehouse to enter, store, analyze, and retrieve all of our risk assessments, audits, time charges, budgets, workpapers, findings, and follow-up entries.

Chapter II - Workpapers & Audit Programs

Once upon a time... We used to print out all our workpapers and sign off on them manually.

But now... Audit Leverage maintains electronic links between audit steps, workpapers, audit recommendations, and review notes. Audit managers can sign off electronically.

Chapter III - Timesheets & Budgets

Once upon a time... We used to fill out timesheets in Excel, then print or e-mail them for approval.

But now... We enter each day's hours directly into Audit Leverage, where our supervisor can approve it electronically and analyze it by audit, by auditor, by time period, and more. Budget-to-actual comparisons tell us where our time is really going.

Chapter IV - Staffing & Scheduling

Once upon a time... Schedule changes caused confusion.

But now... Audit Leverage's Visual Scheduler™ allows us to manage each auditor's calendar and to deal with schedule changes in real-time.

Chapter V - Risk Assessment & Annual Planning

Once upon a time... One year's risk assessment results weren't linked with previous years'.

But now... Audit Leverage lets us use our own risk criteria and recommends an audit plan based on prior years' activity. During the year, it shows us actual progress against our plan.

Chapter VI - Audit Committee Reporting

Once upon a time... We used to waste dozens of hours preparing for an Audit Committee meeting.

But now... We use Audit Leverage to generate those labor-intensive reports that the Audit Committee wants to see.

Chapter VII - Remote Audit Supervision

Once upon a time... My manager had to wait until I returned to the office to review workpapers and time charges.

But now... Audit Leverage's remote synchronization feature allows our audit manager to make mid-course corrections to the fieldwork - before it's too late.

Chapter VIII - Audit Follow-up

Once upon a time... After issuing our audit report, we pasted the findings into a separate follow-up spreadsheet.

But now... When we type our audit findings and management responses into Audit Leverage, it generates the audit report for us - and also tracks our follow-up efforts for each issue.

Chapter IX - Issue Analysis

Once upon a time... Identifying the the most common audit issues meant days of sifting through audit reports.

But now... Audit Leverage's powerful reports provide statistics on the most common audit recommendations by topic, division, region, and more. We can maintain our own library of best practices.

Audit Leverage™ by IAD Solutions

Work happily ever after.

Write your own happy ending. Contact us.
E-mail: info@AuditLeverage.com
Phone: 1-866 AL by IAD (Toll Free) or 215-713-0378
Visit us on the Web at www.AuditLeverage.com

Seven Ways SMEs Can Benefit from GRC Solutions

Dan Wilhelms is president and chief executive officer (CEO) of SymSoft Corp., the makers of ControlPanelGRC, professional solutions for compliance automation *(www.controlpanelgrc.com)*. He can be reached at *dwilhelms@sym-corp.com*.

When the US Sarbanes-Oxley Act was first enacted in 2002 in the wake of several very visible accounting scandals, small to medium enterprises (SMEs) may have felt they dodged a very expensive bullet. The requirement to document processes for governance, risk management and compliance (GRC), and have them confirmed by outside auditors, applied only to publicly traded companies. Unlike their publicly traded brethren, SMEs were not forced to purchase costly GRC software, did not have to redirect resources from their normal daily tasks to prepare for audits and did not have to change their methods of operation to comply with a government mandate.

Yet a funny thing happened in large enterprises as a result of that "bullet." While at first they did it just to check off the "compliance" box on their list of tasks, in time they found that they were operating more efficiently, lowering their costs, driving innovation and becoming more agile. The focus in GRC shifted from the "C" to the "G" and the "R." And as SMEs stood on the sidelines and watched, suddenly the idea of following a GRC regimen started looking more attractive.

> "The focus in GRC shifted from the "C" to the "G" and the "R."

What was not attractive was the price tag for those first-generation GRC solutions. Now, with the introduction of second-generation GRC solutions, the price has come down significantly. In fact, some second-generation GRC solutions are one-third the cost (or less) of the first-generation products.

Still, SMEs are not required to demonstrate compliance to outside auditors or to the government. So how does an organization decide whether the benefits of implementing a second-generation GRC solution outweigh the cost? Here are some things to consider:

1. **Minimizes risk.** Every business, no matter what the size, has risks. Anytime human beings perform manual processes, there is a risk of something being done wrong—either accidentally or on purpose. In a privately held company, those discrepancies are potentially more devastating than they are in a public company. They are also much more personal. A second-generation GRC solution mitigates that risk by automating and regulating business processes. It can assure that all work is performed properly by refusing to allow completion of the process if the prescribed procedure is not followed.
2. **Tightens up business processes.** When a business first starts out, all the rules and business processes are generally laid out and closely followed by everyone who works there. Over time, however, as the business expands, the processes tend to expand along with it. Different people have different ways of working and will tend to do things in the way they are most comfortable—even if it conflicts with the organization's best practices. Second-generation GRC solutions help rein in the "cowboy" approach by tightening up business processes, and then making compliance a part of the process instead of a separate operation. At the same time, if there are improvements that need to be made, they can be easily implemented across the entire organization rather than affecting only the originator(s). Ultimately, they create a culture of controls, ensuring that work is completed by following the proper, repeatable processes rather than through individual acts of heroism.
3. **Improves change management.** Anytime there is a change, it is important to document it to be able to trace back through any later problems. Yet, documentation is often the bane of an organization—something people know they should do but often put off in the interest of more urgent matters. Second-generation GRC solutions automatically create the documentation for any changes, assuring that there is always a current and accurate record of

Do you have something to say about this article?

Visit the *Journal* pages of the ISACA web site *(www.isaca.org/journal)*, find the article, and choose the Comments tab to share your thoughts.

every process from inception on. They also allows SMEs to make more changes within a given time frame, helping them react more quickly to market pressures and opportunities.

4. **Helps drive innovation.** There are only so many hours in the day, and so much work each person in the organization can do. If that time is spent performing manual tasks (such as documenting changes), it is not available for more high-value work. By automating tedious but necessary manual processes, second-generation GRC solutions free up those resources, allowing more time to drive innovation and to help the organization gain a competitive advantage.
5. **Increases agility.** One of the theoretical advantages an SME holds over a large enterprise is agility. Smaller companies are expected to be able to react more quickly to problems as well as sudden opportunities in the market. But, if they are bound by outdated or slow business processes, that advantage is often lost. Second-generation GRC solutions help SMEs regain and even increase their agility, making them more competitive even in the face of factors they cannot control (such as the economy).
6. **Eliminates costly, repetitive tasks in the enterprise resource planning (ERP) landscape.** By their nature, ERP systems have many repetitive tasks. An example could be something as simple as provisioning new users into the system. This is normally a manual task that takes time away from more important work. Yet, it is also the foundation for everything else that user will do in an ERP system, so it is important that it be done quickly and accurately. Second-generation GRC solutions can automate the process of enrolling users, with the appropriate controls and audit trail to assure everything is spot-on. As a result, ERP administrators spend less time on repetitive manual tasks, which frees them to do more high-value work.
7. **Can be implemented in stages.** Unlike the mandatory efforts for publicly traded companies that resulted from Sarbanes-Oxley, use of second-generation GRC solutions in SMEs is completely voluntary. As a result, they can be implemented in stages, allowing the cost savings from stage one to help fund the second stage, and so on. This option makes gaining all the other benefits much more palatable and realistic for budget-conscious organizations.

Compliance may not be required for SMEs, but sound business practices, tight controls and agility are—especially in the current economy. Second-generation GRC solutions give SMEs the tools they need to act like the "big boys"—and reap all the attendant benefits. They also make SMEs more attractive business partners for enterprises that are required to demonstrate compliance. When all the factors are considered, it is apparent that GRC is not the bullet that SMEs thought they dodged, but a powerful weapon to increase competitive advantage. And, now is the time to seize the opportunity.

> "Second-generation GRC solutions give SMEs the tools they need to act like the "big boys"—and reap all the attendant benefits."

EDITOR'S NOTE

Collaborate with ISACA members and access additional resources on this topic in the ISACA Knowledge Center located at *www.isaca.org/knowledgecenter*.

A Case for a Process-based Approach to GRC

S. Ramanathan, CISA, CISSP, has been working in the area of information technology for the past three decades and has worked in several capacities, as a consultant, head of the management information systems (MIS) function and head of the profit center in software companies. He is currently running his own consulting firm, Param Consulting, focusing on IT governance and IT strategy. Ramanathan is a visiting faculty at several of the leading business schools in India. He is an active member of the Computer Society of India and is a regional vice president of the society. He can be contacted at *sram@paramconsulting.com.*

Do you have something to say about this article?

Visit the *Journal* pages of the ISACA web site *(www.isaca.org/journal)*, find the article, and choose the Comments tab to share your thoughts.

A number of corporate accounting scandals, such as Enron, created a need for regulations, such as the US Sarbanes-Oxley Act. The need for sound corporate governance principles was actively debated in this context, and the concept of governance, risk management and compliance (GRC) resulted. The concept has wide coverage now, encompassing enterprise risk management (ERM), operational risk management, incident management and other related areas. As with many popular concepts and practices, there are myths surrounding GRC, too. Some of these myths include:

- GRC is for the board to worry about; day-to-day management is not concerned with GRC.
- GRC is for big companies only.
- GRC is for listed companies to worry about.
- GRC is a pain organizations have to live with because government wants it.
- GRC is about documentation and reporting.
- GRC implementation interferes with the business.

Irrespective of size and pattern of ownership, organizations need to recognize that governance is the superordinate requirement to sustain ongoing activities, and risk management and compliance are necessary prerequisites for ensuring good governance. Thus, GRC needs to be a critical concern for all organizations, and its focus should be much larger than statutory compliance.

A narrow focus has made GRC a reactive and piecemeal exercise in organizations. Even larger organizations with a better vision of GRC take up statutory compliance as the first step, and the larger exercise of holistic implementation and maintenance of GRC is placed at a lower priority. Consultants who are engaged in these assignments are forced to cater to the immediate needs of management and, thus, fail to present a comprehensive approach of ERM as part of GRC.

The subject of this article is to present a more fundamental approach to GRC and to suggest the most appropriate methodology to make the exercise sustainable. Such an approach puts additional responsibilities on information systems (IS) auditors as well (this is addressed toward the end of the article).

Typical GRC implementation approaches include:

- **Checklist-based**—For reasons cited previously, organizations implement GRC as a reporting exercise. Implementers and auditors adopt the checklist approach[1] for testing compliance to a list of requirements.
- **Asset-based**—In this method, information assets and their vulnerabilities are identified. Threats that could compromise confidentiality, integrity and availability of these assets are then identified. Based on the probability of threats exploiting these vulnerabilities and the consequential impact, the risk exposure is computed. Risk mitigation measures are suggested for vulnerabilities with risk exposures higher than the risk tolerance limit. The methodology is the application of Failure Mode and Effects Analysis (FMEA),[2] popular in engineering design and analysis, to the IT domain, except that FMEA does not recommend an asset-based approach. Though the International Organization for Standardization (ISO) does not recommend any specific method for information security assessment, consultants and practitioners have been using this method for ISO 27001 implementation.[3] The Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) method, developed by the Software Engineering Institute (SEI), is another asset-based method.[4, 5]
- **Incident-based**—Another approach that is recommended for risk management and audit is to look at the past deviations, using incident reports, error reports, system failure reports, etc. Using loss-event data collection as a measure of operations risk exposure, as recommended by Basel II,[6] is an example of an incident-based approach.[7]

A checklist-based approach is environment-specific and lacks rigor. However, this approach is popular for audits because of its simplicity. It is useful for regular periodic audits and serves the purpose when there has not been any major change in the business processes.

An incident-based approach assumes that if there is a problem in the system, it would be visible in some of its effects. To what extent is this true? To take an analogy of the human body, a viral infection would manifest in symptoms such as a cough and a cold, so monitoring external symptoms could unearth the underlying malady, but there could be a possibility that some dormant phenomenon such as cell mutation could go undetected until it develops into cancer. Incidents provide clues to the level of exposure and allow organizations to recalibrate their business processes to meet the new exposure levels.[8] But, if the incident turns catastrophic, it is too late for any remedial action. The recent collapses of several financial institutions despite implementation of Basel II recommendations are examples; these collapses did not leave any time for recomputation of capital requirements.[9]

An asset-based approach is more rigorous and comprehensive than these two approaches. In this approach, risk is looked upon as a threat to an asset, and the remedial measures are incorporated in the business processes of the organization. In the subsequent sections, an argument is presented that instead of looking at the processes for remedial action only, one needs to apply a rigorous analysis to the process(es) associated with the management of assets.

The argument is based on the premise that incidents or threats to assets are due mainly to process vulnerabilities. These vulnerabilities could arise due to poor design of processes or controls associated with these processes or due to their improper implementation. Hence, a fundamental approach to risk analysis should start with process analysis.

> "A fundamental approach to risk analysis should start with process analysis."

PROCESS-BASED APPROACH: EXPLAINING THE RATIONALE

Risks arise because of exploitation of a vulnerability in the process. During a given period, a vulnerability may or may not result in some form of damage to an asset. It may or may not show up as an incident. Regardless, the fact remains that the vulnerability exists, ever ready to be exploited. When a risk emerges and becomes conspicuous to the users, it may have already caused damage to the processes/assets of the organization; therefore, any attempt to address risks without studying the vulnerabilities would amount to remedying the consequences without addressing the causes. That is why it is advised that the processes need to be studied for their vulnerabilities. The reason many frauds are perpetrated by internal people is because of their knowledge of vulnerabilities in the business processes.

The suitability of a process-based approach can be appreciated through a case example: A large chemical manufacturing organization had a problem in which many vendor checks were returned because of spelling mistakes in the name of the vendor. The vendor master had 4,000 entries, and the uncontrolled entry by many assistants had led to several names being misspelled. Since spelling mistakes did not create any problem in order execution, the purchase department, owner of the table, did not take any measure to correct the table. Accounts requested a facility for correcting the names while preparing checks. This was approved by management. While trying to address recurrent vendor complaints and associated problems, management did not realize that they were introducing a control weakness. No violation was reported during the six months in which this procedure was occurring; therefore, incident-based audit failed to capture the vulnerability. Asset-based risk assessment showed the vendor check returns as a threat to company reputation, an important asset, and the name correction facility for the accounts as an alleviation measure, thus the assessment showed reduced risk. It was only when the process was analyzed that the risk introduced became apparent.

PROCESS-BASED APPROACH: AN OVERVIEW

A process view of an organization is a very detailed view and requires progressive elaboration until all elemental tasks are identified. Insiders in an organization would have only a partial/gross-level view of the processes and, thus, may not be fully aware of the vulnerabilities in the processes. A detailed documentation, mapping all business processes at their elemental level, is a necessary first step. Many vulnerabilities arise at the interprocess interface level and, thus, get omitted when processes are mapped in an isolated manner by their respective owners. The level of details required

for documentation of all the business processes makes it a daunting and cumbersome task that many organizations are hesitant to undertake.[10] But, this is a onetime task that organizations need to complete, after which the process maps need to be maintained. The latter is a manageable task if undertaken on an ongoing basis.

A structured way of understanding an organization is to take a hierarchical view of the processes. This would help one understand the relationship of the processes to the business goals as well as the interrelationship among the processes. Hierarchy starts with deliverables in terms of products/services, and then the associated business processes for these deliveries are identified. Processes need to be decomposed into subprocesses and activities. The process map is complete only when the following have been identified:

- The roles that perform each of the tasks
- Entities, including assets, impacted by the processes
- Application programs affecting the process
- Data (tables) affected by the process
- Documents used by the process (data and documents used by this process would provide a link to the process that generated the data/documents)
- Documents generated by the process
- Controls built into the process

The controls built into the process give an idea of the risks identified, and the process analysis should include the residual risk after the controls.

AUDIT

The process-based approach puts additional responsibilities on GRC auditors, too. GRC auditors should take a process view and check the processes. Obviously, the auditor has to undertake a sampling test to conduct the audit. While selecting processes for audit, some or all of the following criteria may be applied:

> "The process-based approach puts additional responsibilities on GRC auditors."

- Criticality of the process to the business
- Financial implication of the process
- Processes involving outsider interaction
- Customer interaction processes
- Recently changed processes

Depending on the level of maturity of processes, criticality of business and frequency of audit, the auditor may decide to perform a substantive audit to check the robustness of the processes as mapped or a compliance audit to check the match among the practices and processes.

In organizations in which extensive documentation of the processes exists, the auditor needs to check the conformance of the process document to the process in practice. If there are deviations, the process map has to be changed, and then the process needs to be analyzed for its robustness. This check has to address the following queries:

- What are the process objectives?
- How are they aligned to business objectives?
- What are the sources of data for this process? Are these data authenticated?
- What are the direct data entries into this process? How are they authenticated?
- What are the checks built in the process? What are the stated objectives of these checks? Are they sufficiently robust to achieve the desired objective?
- Which are the roles that hold data entry/modification rights in the process? Do these roles have sufficient authority to perform these actions?
- What are the implications of such data change/wrong data entry?
- What are the checks available for entry of accurate, authorized data only?

This is an indicative checklist and needs to be modified depending on the process and the context.

Where process maps do not exist, the auditor has the challenging task of preparing the maps for the processes identified for audit. Audit firms may need to build in-house expertise in developing business process maps or usage of business process management (BPM) tools.

AN EXAMPLE

The following banking example[11] is provided to help explain the four-step process-based approach:

1. Business processes are designed in an organization with a view toward delivering a product/service. Therefore, in a top-down approach, identify the products/services delivered by the organization (see **figure 1**).
2. Identify the business processes associated with each of the products/services. This example takes personal loans as the product example and maps their business processes (**figure 2**).

3. Take the presanction subprocess and expand it (**figure 3**). This step can iterate several times until the elemental level of tasks is reached. While mapping the subprocesses/activities, also map the following:
   - Roles associated with the subprocess/activity (shown in gray rectangles in **figure 3**)

Figure 1—Products/Services

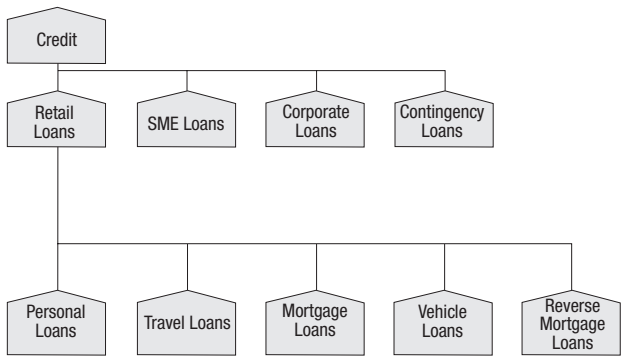
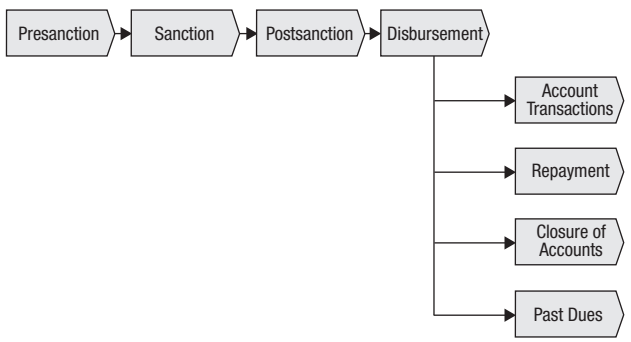


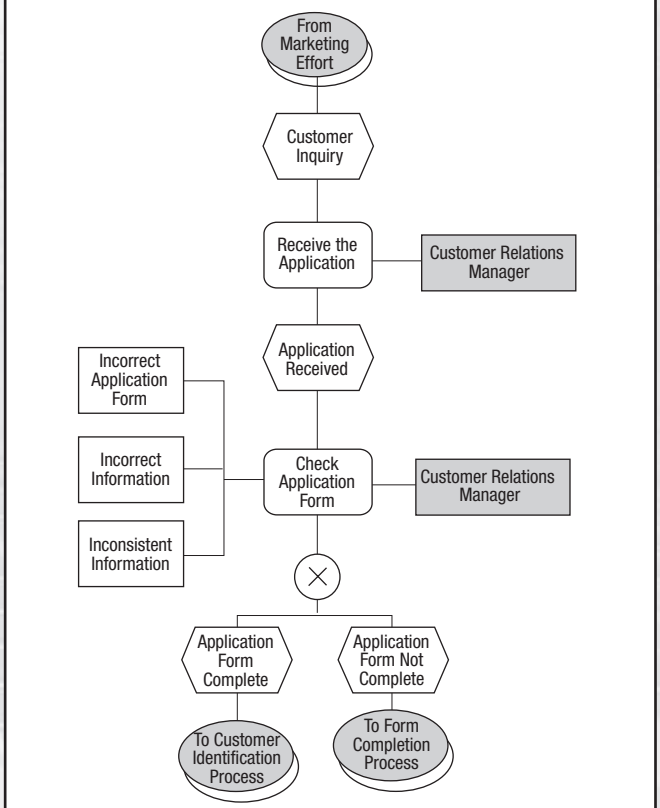
Figure 2—Personal Loans Business Process



   - Entities/documents associated with that subprocess/activity (e.g., application form)
   - Risks associated with the subprocess/activity (shown in gray ovals, in **figure 3**)

   During an audit, the auditor has to independently draw the map for risks and ensure that all risks have been identified by the process owner.
4. For each of the risks identified, map the controls (**figure 4**). During the audit, the auditor should check that, for all identified risks, the controls available are adequate.

Figure 3—Presanction Subprocess Expanded

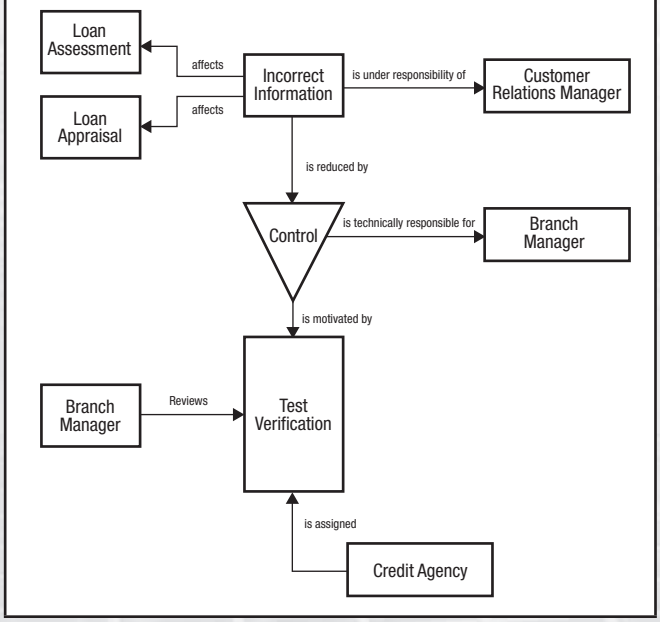


CONCLUSION

This article reviews different risk analysis approaches and argues that a process-based approach addresses the requirements from the basic details and, hence, is more rigorous and comprehensive. The GRC approach has evolved beyond Sarbanes-Oxley compliance, and the GRC tools are maturing to address comprehensive risk management needs. There are process-based GRC tools currently available in the market.[12]

A sound GRC model would mandate the maintenance of a business process maps repository in the organization. The challenge lies not only in creating and storing these maps, but also in maintaining them. In a dynamic market situation, organizations keep adding products and services. Market demands compel organizations to continuously improve their business processes to suit the newer products and services. Even organizations that offer a fixed portfolio of products

Figure 4—Controls Mapped for Each of the Risks Identified



and services need to innovate their business processes to maintain their agility and competitiveness. These changes need to be reflected in the business process maps, and a good configuration management of these maps is essential.

Auditors should also redefine their process-based approach and should build the necessary competencies to fulfill this task. Irrespective of the organization's approach toward GRC implementation, auditors should undertake a process-based approach, as this addresses the risk at the most elemental level and is, thus, more comprehensive. This approach has already gained popularity among larger consulting and audit firms because of its strengths.[13]

ENDNOTES

1 There are checklists made available by popular software vendors such as SAP and Oracle. Consulting organizations develop and use checklists based on their experience.

2 A detailed discussion on this technique can be found at the FMEA Info Centre site, *www.fmeainfocentre.com*.

3 The implementation approach can be seen on any of the ISO 27001 consultant sites. For example, *www.hsc.fr/services/accompagnement27001.html.en* is one such site that recommends an asset-based approach for risk assessment.

4 Panda, Parthajit; "The OCTAVE Approach to Information Security Assessment," *ISACA Journal*, vol. 4, 2009

5 The framework document explaining the approach is available at *www.sei.cmu.edu/library/abstracts/reports/99tr017.cfm*.

6 Bank for International Settlements, *Basel II: International Convergence of Capital Measurement and Capital Standards: A Revised Framework—Comprehensive Version*, Switzerland, June 2006. It devotes one section to loss data. See clauses 670-673.

7 Girling, Phillippa; "Practical Operational Risk Management Part Four—Loss Data Collection," Complinet, 5 May 2009, *http://www.garritygraham.com/CM/Custom/Part-4.pdf*

8 Nir, Karen; Sumit Anand; Sam Mannan; "Calibrate Failure-based Risk Assessments to Take Into Account the Type of Chemical Processed in Equipment," *Journal of Loss Prevention in the Process Industries*, May 2006. While this article deals with risk in chemical processes, the underlying concept of incident-based risk assessment is applicable to business processes as well.

9 This issue has been reviewed critically, though not extensively, by Harald Benink and George Kaufman in "Turmoil Reveals the Inadequacy of Basel II," *Financial Times*, UK, 28 February, 2008. The authors forcefully argue for a revised approach for capital computation in view of the financial sector collapses.

10 This is one reason why a good BPM tool should be used. As of 2009, Gartner identifies 22 major vendors for BPM tools (Hill, Janelle B.; Michele Cantara; Marc Kerremans; Daryl C. Plummer; "Magic Quadrant for Business Process Management Suites," Gartner RAS Core Research Note G00164485, 18 February 2009).

11 The author thanks V. Ganesh, an experienced banker and consultant with Thesys Technologies, Chennai, India, for providing valuable inputs for creating an example.

12 For example, BWise and ARIS are two popular process-based GRC software tools.

13 Bevis, Jason; "What Is Better? Process or Asset Risk Assessment?," *InfoSecAlways.com*, 11 March 2007

EDITOR'S NOTE

Collaborate with ISACA members and access additional resources on this topic in the ISACA Knowledge Center located at *www.isaca.org/knowledgecenter*.

Prepare for the **2010** CISM Exams

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

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

www.isaca.org/cismreview

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

CISM Review Manual 2010

ISACA

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

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

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

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

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

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

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

CISM Review Questions, Answers & Explanations Manual 2009

ISACA

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

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

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

CISM Review Questions, Answers & Explanations Manual 2009 and 2010 Supplements

ISACA

Developed each year, the *CISM® Review Questions, Answers & Explanations Manual 2009 Supplement* and *2010 Supplement* are recommended for use when preparing for the 2010 CISM exam. Each supplement consists of 100 different sample questions, answers and explanations based on the current CISM job practice areas, using a process for item development similar to the process used for developing actual exam items. The questions are intended to provide CISM candidates with an understanding of the type and structure of questions that have typically appeared on past exams, and were prepared specifically for use in studying for the CISM exam.

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

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

CISM Practice Question Database v10

ISACA

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

PLEASE NOTE the following system requirements:
- 400 MHz Pentium processor or equivalent (minimum); 1 GHz Pentium processor or equivalent (recommended)
- Supported operating systems: Windows Server 2003, Windows Server 2008, Windows Vista, Windows XP
- 512 MB RAM or higher
- One hard drive with 250 MB of available space (flash/thumb drives not supported)
- Mouse
- CD-ROM drive

MDB-10 English Edition—CD-ROM
MDB-10W English Edition—Download

Risk-based Approach to IT Systems Life Cycle and Change Control

Loic Jegousse, CISA, CISM, is the director of IT standards, compliance and internal controls with MDS Inc., a global life sciences organization. Jegousse has spent his 11-year career in technology risk consulting and audit in global industries such as financial services, life sciences and professional services. His specializations include IT controls, regulatory compliance, information security, IT governance, IT outsourcing and process improvement.

"If one is forever cautious, can one remain a human being?"
—Aleksander Solzhenitsyn

The human brain is inadequately trained to manage risk effectively: Countless people continue to smoke tobacco, drive without a seatbelt and engage in other hazardous behaviors. Individuals may accept unreasonable risk (e.g., get a loan while already indebted to invest on a speculative investment) if it can yield a higher payoff.

Running against human nature, regulatory and governance pressures—e.g., the US Sarbanes-Oxley Act, Basel II, International Organization for Standardization (ISO) standards—are prompting management to systematically identify significant risks and mitigate their impact. In risk management literature, risk is seen as a function of the probability of occurrence and impact. These are difficult to assess with precision. In real life, humans tend to underestimate ("accept") risks that have a low or remote probability of occurrence (even those that could have a catastrophic impact) for reasons including scarcity of resources (especially time) and tendency to focus on short-term objectives. In the business and technology world, managers struggle to implement sustainable and cost-effective means to balance risks and operational constraints.

BALANCING EXERCISE

This article explores the concepts of a risk management model in the context of change management to IT systems, and their ramifications with respect to system life cycle controls. However, the model and its concepts could be applied to other business risk areas. **Figure 1** illustrates a practical, risk-based approach to IT systems that proposes a balance between two extreme models (noncompliant vs. highly compliance-focused). This approach is aiming to deliver:

- Documentation and system validation efforts commensurate with the risk
- A repeatable, measurable and scalable IT risk assessment process over IT systems
- Sustained compliance with regulatory requirements

The main critique of the highly compliance-focused approach is that it is resource-consuming and difficult to apply consistently. In real life, an illustration of such an approach applied to the airline industry would be that all components of the aircraft, as well as passengers and staff, would be thoroughly and consistently checked for structural damage, identity of passengers would be checked, inspection of luggage would be conducted, etc. All possible scenarios that could compromise safety (e.g., liquids, hidden explosives, collusion with staff) would be examined, ranked and managed accordingly in a series of standard procedures and checklists. Such conservative approaches, while robust on paper, are not necessarily sustainable in the long term, as large costs would be involved.

At the other end of the spectrum, a noncompliant approach would involve a highly judgmental, undocumented and subjective assessment of risks. In the airline analogy, the unstructured control would be left to airline crew screening sample passengers via an informal procedure, e.g., using observation and simple inquiry only. Such an approach would cause unreasonable acceptance of risk to passengers' safety and would understandably cause public concerns.

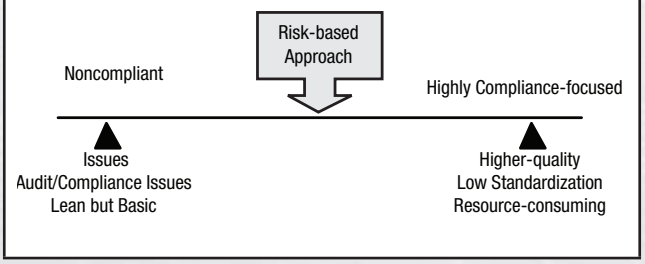
REDEFINING RISK

When it comes to IT systems life cycle and change control, there is often some confusion as to how to comply with certain regulatory requirements relating to computerized systems, without producing massive amounts of documentation for a simple change or a large implementation project. For instance, publicly traded

Do you have something to say about this article?

Visit the *Journal* pages of the ISACA web site *(www.isaca.org/journal)*, find the article, and choose the Comments tab to share your thoughts.

Figure 1—Balance Between Noncompliant and Highly Compliance-focused Approaches



organizations encountered an excessive paperwork burden during the first years of enforcement of the US Sarbanes-Oxley Act requirements for systems that were remotely related to financial reporting. Other examples are the "good practices" from the US Food and Drug Administration (FDA), which require computerized systems to be maintained in a validated state.

Taking, as an example, a complex business application, such as an enterprise resource planning (ERP) system, for which code changes or extensions occur frequently, some areas of the application system, such as payroll, cash management or general ledger, are subject to a higher level of data integrity and system security. When a particular change is made to an application system or its supporting hardware components, how can management ensure that it will not have any unforeseen negative impact on certain functionalities or data? On the one hand, IT could take a hands-off approach and hold the business users accountable for data integrity. Such a noncompliant approach could rapidly cause soaring audit costs, regulatory issues and lack of trust toward the systems. On the other hand, performing extensive validation, regression testing and documentation for the entire system every time a change is made to ensure that everything works as expected can be expensive and would not be sustainable in the long term. There needs to be a compromise between these two models. The solution is to use a risk assessment framework that will assist in simplifying the degree of system life cycle controls relative to perceived risks.

RISK ASSESSMENT FRAMEWORK

The proposed risk-based approach to IT systems is based on classes of risk (hereafter referred to as risk factors). The value of the risk factors relates to a situation that has a combined probability and impact value, which can be expressed as a monetary value (e.g., net present value) or in a qualitative manner. Risk factors are to be defined based on the potential damage to the organization, as well as the existence of predetermined methods that can be used to reduce the damage. As an example, this article further details a two-dimensional model that involves the following risk factors:

- **Business**—A situation that may result in loss of productivity, financial loss, liability or reputation damage, if it is not managed effectively. An example of a risk mitigation method to reduce business risk would be to increase management oversight of the activities.
- **Regulatory**—A situation that may modify the configuration of key automated controls that support compliance with regulatory requirements (e.g., controls over financial reporting or other key business processes such as privacy, drug or medical device safety). An example of a risk mitigation method to reduce regulatory risk resulting from data integrity issues would be to increase the depth and breadth of system life cycle artifacts.

To operate such a process, management needs to develop explicit criteria to define what the low, medium or high risk ratings mean. For instance, in the context of regulatory risk, high risk criteria are defined per an explicit list of systems controls that are subject to regulatory requirements. Low risk criteria include instances with a very remote likelihood to modify the integrity, availability or confidentiality of records or sensitive data. Each risk factor is assessed for a low, medium or high value. The results are then plotted on the risk level chart, which returns the resulting risk level (e.g., 1 to 4), as shown in **figure 2**.

RISK MITIGATION STRATEGIES

The risk levels are defined in a manner to provide a higher level of management oversight as the business risk factors increase. As an illustration, the risk levels may be defined as shown in **figure 3**.

In addition, the resulting risk levels involve an increasing amount of system life cycle controls, as the regulatory risk factors increase. This would include increased effort with respect to system documentation, testing and code review. **Figure 4** is an illustration of the relationship between the risk levels and the typical documentation deliverables required for various stages of the process/life cycle (e.g., design, testing, promotion, validation).

Figure 2—Risk Level Chart

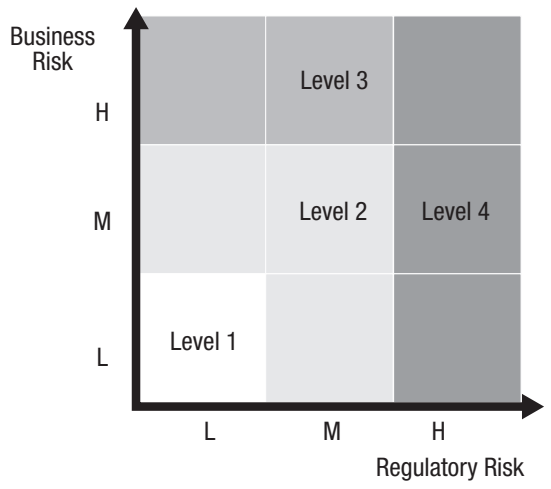


Figure 3—Risk Levels for High Business Risk Factors

Risk Level	Management Oversight
Level 4	All members of the IT leadership team plus one member of quality assurance/compliance/audit, etc., function
Level 3	All members of IT leadership team
Level 2	One member of IT leadership team
Level 1	One manager of IT

Figure 4—Risk Mitigation for High Business Risk Factors

Risk Level	Stage A (e.g., formal specs)	Stage B (e.g., formal testing)	Stage C (e.g., change control form)	Stage D (e.g., validation report)
Level 4	Required	Required	Required	Required
Level 3	Required	Required	Required	Discretionary
Level 2	Discretionary	Required	Required	Discretionary
Level 1	Discretionary	Discretionary	Required	Discretionary

CRITICAL SUCCESS FACTORS

The risk-based approach should be supported by standard operating procedures (SOPs) to provide instructions and training to the affected personnel. Frameworks such as COBIT, IT Infrastructure Library (ITIL) and Good Automated Manufacturing Practices (GAMP) provide high-level requirements for the design of IT processes over the system life cycle, application management, access control and change control.

When designing a risk-based approach, it is important not to underestimate the effort required in performing an accurate inventory of automated systems functions or situations that are linked to high risk factors. This inventory is the backbone of the risk-based procedure, and its accuracy and simplicity will enable an effective process. A key success factor is the adequate involvement and support of the various quality assurance, privacy, legal, audit, regulatory affairs or compliance teams in high regulatory risk situations. Some IT system changes may, based on risk ratings, require sign-off from key stakeholders before proceeding.

CONCLUSION

Organizations that have successfully implemented risk-based approaches have observed cost savings, cycle time and customer satisfaction improvements. Management can appreciate that lower risk change requests can be processed swiftly, while still demonstrating the rigorous analysis that was performed to justify a low risk level. In addition, key stakeholders (even outside of IT) are now systematically consulted before approving system changes that are deemed as higher risk. Such an approach can also deliver increased governance over those particular risks that are not tolerated within the organization.

EDITOR'S NOTE

Collaborate with ISACA members and access additional resources on this topic in the ISACA Knowledge Center located at *www.isaca.org/knowledgecenter*.

Manage Requirements Volatility to Manage Risks in IS Development Projects

Sachidanandam Sakthivel, Ph.D., is a consultant in IT outsourcing and information systems development methods. Sakthivel has published numerous articles in leading international journals. He has also presented numerous articles at international conferences and is a member of the Association for Computing Machinery (ACM) and the Institute of Electrical and Electronic Engineers (IEEE).

Requirements volatility (RV) refers to additions, deletions and modifications of requirements during the systems development life cycle. RV creates rework in design and code that increases the system development cost and time and compromises the system quality. Ignoring requests for requirement changes can cause system failure due to user rejection, and failure to manage RV can increase the development time and cost.

A meta-analysis of several studies shows that system development projects have an average of 25 percent time overrun and 41 percent cost overrun.[1] RV is the cause of failures in about 11 percent of system development projects.[2, 3] Information systems (IS) professionals consider RV a critical risk. The management of RV is essential to success in a systems development project.[4]

This article discusses the risk factors for RV, suggests methods to manage RV to reduce project risks, and relates RV and its management to various control objectives in COBIT.[5]

RISK FACTORS FOR RV

Strategic IS have an inherent risk for RV because such systems are new to a firm and possibly not implemented by any other company in the industry. Requirements for such systems are initially unclear and evolve over time. Since new technology takes time to evolve and mature, such technologies in systems can cause RV. Users' inadequate knowledge of technology and developers' inexperience with technology are additional sources of RV. Large systems with a large number of requirements have scope for many changes. Large systems without adequate user representation of all concerned departments can produce incomplete requirements that will be added later or incorrect requirements that will be corrected later. In complex systems, a change in requirement may start a chain reaction to cause more requirement changes, some of which may be missed and corrected later.

Another risk factor for RV is with unique and differentiated business processes that have unclear requirements initially and that evolve during development. Since system development is knowledge-intensive collaborative work, insufficient user knowledge of the application may lead to poor articulation of requirements that will need changes later. Similarly, if developers have insufficient knowledge of the application domain, they may not fully understand user requirements that will need changes later. Frequent turnover of developers and/or users in the development team will affect continuity and lead to changes in requirements. Projects that are forced to be completed earlier than the required time may lead to an incomplete and incorrect requirements definition and subsequent changes. Finally, users may add, modify or delete requirements due to lack of planning on their part or due to indecisiveness. **Figure 1** summarizes various risk factors for RV.

Figure 1—Risk Factors for RV

- Strategic information systems
- New technology
- Developers' inexperience with technology
- Lack of users' knowledge of technology
- Large systems
- Complex systems
- Unique/differentiated business processes
- Users' inadequate knowledge of application
- Developers' inadequate knowledge of application
- Many departments/functions in the system
- Unstable project team
- Compressed project schedule
- Nonessential requirement changes

Recognizing any of these RV risk factors in a proposed systems development project can help to manage the consequent project management risks. Specifically, recognizing these risk factors would help in assessing the IT risks as in process PO9,

Assess and manage IT risks, in the Plan and Organize (PO) domain of COBIT. The next section discusses the responses to RV risks and the management of such risks.

RV RISK MANAGEMENT METHODS

RV is a risk believed to be uncontrollable and outside of a project manager's influence.[6] Although not all RVs can be controlled, they can be managed. Project managers can reject requirement changes that are not critical to achieving a system's objectives, they can create a development environment that eliminates the causes for avoidable RV and they can use development methods that work with volatile requirements. Finally, where such methods are not feasible, methods to manage the RV and the consequent changes in design, development and implementation are essential. The following sections discuss methods to manage RV risks.

Reject RV

The easiest suggestion to manage RV is to freeze the requirements and reject the volatility. However, this may not be practical in many situations because users may reject the system without the changes. In addition, the expected system benefits may not be achieved without the requirement changes. A project manager may not be able to prevent the RV in systems that are controlled by project stakeholders at a higher level. Nevertheless, the manager may have freedom with the requirements of nonstrategic systems. In these systems, the manager can separate the essential requirements from useful and nice-to-have requirements and be able to freeze the nonessential requirements. However, the manager should have the authority to reject a requirement change, unless it is critical to achieving the system objectives, and to prevent the volatility of nonessential requirements.

Eliminate Avoidable Causes of Volatility

A previous section discussed factors such as unique and differentiated business processes in an information system that would have unclear requirements initially and that would evolve during development. A solution to deal with such volatility is to avoid unique and differentiated business processes that do not have major benefits in nonstrategic systems. It is better to migrate to standard and accepted business processes in such cases. Where it is not possible to avoid such unique processes, process experts should be co-opted to identify requirements correctly and completely.

Volatility created by new technology and inexperience with current technology can be reduced or avoided by co-opting technology consultants in the requirements definition process. The development team should include users and developers with knowledge in the application domain to avoid incorrect and incomplete requirements that will be changed later. Volatility caused by users' insufficient knowledge of an application can be balanced by having process experts on the development team.

RV due to inadequate user representation of various functions can be minimized by having the right number of users to represent each function. Having a stable team of developers and users on the development team will ensure continuity and avoid requirement changes that come with new team members.

Structured definition methods are useful when documenting and managing requirements. These methods can also help to update volatile requirements correctly and completely to avoid further volatility. Verification and validation of requirements using inspections, reviews and walk-through exercises can ensure that requirements are correct, consistent and complete, and they can help to avoid changes to requirements during later stages.

Use Methods to Work With Volatility

The RV associated with strategic systems and new technology cannot be rejected or avoided. It is prudent to use appropriate requirement gathering and development methods with such systems. Iterative methods such as rapid application development (RAD) and agile development have been found to be useful in the development of systems that have RV, but these methods are not proven for large systems development. In these cases, a prototype can be developed iteratively and used to elicit clear requirements during the requirement definition stage. Prototypes and pilot projects are useful in resolving requirement uncertainties in strategic systems and in systems with new technologies. If developers do not have much experience with the technology, consultants and process experts should be co-opted to identify requirements.

The methods discussed in the previous three sections—methods to reject, eliminate or work with the risks—are consistent with control objective PO 10.9, *Project risk management*, in the PO domain of COBIT.

Manage Volatility and Its Effects

RV increases development cost and time, and, thus, its implementation needs to be managed carefully. An incorrect implementation of requirement changes may lead to more volatility and higher costs. A change management system is essential to identify the impact of a requirement change on cost and schedule as well as on other requirements and system objectives. Changes that have a big impact need to be approved by a committee of senior managers from the user departments and the project sponsor. Current change management methods focus largely on design and code artifacts and very little on the requirements. Structured requirement definition methods can help to trace a requirement to the system's objectives and to determine the impact of a requirement change on system objectives.

Top management commitment is the number one requirement for a project's success. Top management support is essential in resolving conflicts that arise between users and in managing the associated volatility. Both the project and the project manager should have the support and commitment of top management in dealing with requirement changes and in using the RV management methods. These methods to manage the implementation of requirement changes map well to COBIT process AI6, *Manage changes*, in the Acquire and Implement (AI) domain.

Figure 2 summarizes methods that can be used to manage RV risks.

Before executing a systems development project, the project manager should identify various RV risks discussed in the previous section and summarized in **figure 1**. Depending upon the RV risk factor for the project, appropriate risk management methods as indicated in **figure 3** should be adopted. Please note that management methods—such as getting top management commitment, arming the project manager with sufficient authority, verifying and validating requirements, and staffing the project with users and developers who are knowledgeable in the application area—are good practices that are essential in all types of systems development.

Project managers and IS developers are generally aware of risks due to RV, but other project stakeholders may not be aware of various RV risks and the implications of these risks.[7] The project manager has the responsibility of communicating the RV risks to project stakeholders and in educating them in the management of these risks. The project manager and the head of IS development are jointly responsible for identifying and assessing the RV risks in consultation with the owner of the business process, architects of the system, IT administrators, and the information system audit and control group. They are responsible and accountable for identifying

Figure 2—Methods to Manage RV Risks

General Methods	#	RV Risk Management Methods
Reject requirement volatility.	1	Freeze requirements and reject volatility.
Eliminate avoidable causes.	2	Avoid unique processes in nonstrategic systems.
	3	Use technology consultants.
	4	Use process experts.
	5	Ensure that all functions have adequate representation.
	6	Use structured requirement definition methods.
	7	Have a stable development team with low turnover.
Use methods to work with volatility.	8	Use pilot projects and prototypes in requirements analysis.
	9	Use iterative development methods.
Manage volatility and its effects.	10	Use a change management system.
	11	Use conflict resolution methods.
Elements that are essential to the success of all systems development projects:	• Top management commitment • Project manager with sufficient authority • Verification and validation of requirements • Users/developers with knowledge of the application domain	

Figure 3—Guidelines to Manage RV Risks				
	Then Employ These Methods (#s shown in Figure 2)			
If the proposed information system project…	Reject RV	Eliminate Avoidable Causes	Use Methods to Work With Volatility	Manage Volatility and Its Effects
Is strategic in nature		3, 4, 5, 6, 7	8, 9	10, 11
Employs new technology		3	8, 9	10
Has developers without much experience with technology		3	8	
Has users with little knowledge of technology			8, 9	
Is large		7		10
Is complex		6	9	10
Has unique/differentiated business processes		2, 4, 6		10
Has users with inadequate knowledge of an application		2, 4		
Has developers with inadequate knowledge of an application			8, 9	
Involves many departments/functions		5, 7		10, 11
Has an unstable team		7		
Has a compressed project schedule	1		9	10
Gets requests for changes in nonessential requirements	1			

and implementing methods to manage these risks. As the project progresses, the project manager is also responsible for keeping the chief information officer (CIO) and chief financial officer (CFO) informed of the management of RV risks and the impact of the risks on the project outcome.

CONCLUSION

The guidelines discussed in this article help to manage not only the RV risks in in-sourced system development projects, but also help to manage several other risks in these projects. For example, new and unique business processes should be avoided in nonstrategic systems because they not only create RV, they also create a risk of higher development costs without the concomitant benefits.

Outsourced projects would have additional risk factors for volatility of requirements. For example, outsourced projects with time and material contracts have a risk of higher volatility compared to fixed-price contracts. This may be due to vendors expanding the scope of a project to increase their revenue. Globally outsourced projects would have more RV risks due to separation of users and developers in distance and time and due to communication barriers created by language and culture. These types of projects warrant additional RV risk management methods.

ENDNOTES

[1] Lamswede, A.; "Requirements Engineering in the Year 00: A Research Perspective," Proceedings of the 22nd International Conference on Software Engineering (ICSE 2000), ACM Press, Ireland, 2000

[2] The Standish Group, "Extreme CHAOS," USA, 2001

[3] Molokken, K.; M. Jorgensen; "A Review of Surveys on Software Effort Estimation," IEEE International Symposium on Empirical Software Engineering (ISESE 2003), Italy, 2003

[4] Thakurta, R.; F. Ahlemann; "Understanding Requirements Volatility in Software Projects—An Empirical Investigation of Volatility Awareness, Management Approaches and Their Applicability," 43rd Hawaii International Conference on System Sciences (HICSS 2010), USA, 2010

[5] IT Governance Institute, COBIT 4.1, 2007, *www.isaca.org/cobit*

[6] Tiwana, A.; M. Keil; "The One-Minute Risk Assessment Tool," *Communications of the ACM*, vol. 47, issue 11, 2004

[7] *Op cit*, Thakurta

FISMA 2010: What It Means for IT Security Professionals

Tarak Modi, CISA, CISSP, PMP, principal architect at G&B Solutions, is a seasoned business leader, skilled enterprise architect and published author with more than 15 years of experience solving business problems by aligning business and IT. He has coauthored *Professional Java Web Services* and written more than 80 articles related to IT management and transformation. Modi currently leads the cloud computing and security certification and accreditation (C&A) practices within G&B.

New threats related to cybersecurity are causing a shift in focus from compliance to risk-based protection, resulting in new requirements for system security and contingency plans, a greater push for continuous monitoring, and a stronger emphasis on configuration management and incident response.

ARE YOU READY?

The US Federal Information Security Management Act (FISMA), originally enacted in 2002 and currently undergoing considerable revision, establishes clear criteria to improve US federal agencies' cybersecurity programs. But, even as federal agencies struggle to implement their existing information security programs, cybersecurity breaches have become increasingly common, with a 200 percent hike in such breaches over the past three years, according to numbers from a recently released Government Accountability Office (GAO) report in which the number of cybersecurity breach-related incidents reported by US federal agencies has risen from 5,503 in fiscal year 2006 to 16,843 in 2008.[1]

This article looks at how FISMA and its family of key National Institute of Standards and Technology (NIST) Special Publications (SPs) are changing to meet the challenges posed by increasingly elusive hackers who are using better and more sophisticated tools and techniques to attack increasingly lucrative targets. Complacency is definitely not an option. The only option is to stay one step ahead of the game.

BACKGROUND

"It is no secret that terrorists could use our computer networks to deal us a crippling blow," then-US Senator Barack Obama said in July 2008. A report[2] issued by the GAO states that "federal agencies are facing a set of emerging cybersecurity threats that are the result of changing sources of attack, increasingly sophisticated social engineering techniques designed to trick the unsuspecting user into divulging sensitive information, new modes of covert compromise, and the blending of once distinct attacks into more complex and damaging exploits." Such damaging exploits include increasingly sophisticated malware such as worms and viruses and the increased attack capabilities of blended threats and bots.

FISMA is the centerpiece of all of the US laws that have been enacted and implemented over the years to improve the US federal government's ability to thwart cybersecurity attacks. At its core, FISMA requires federal agencies to implement a comprehensive agencywide, risk-based approach to protecting the confidentiality, integrity and availability (CIA) of federal information systems and to protecting information against cyberattacks. To this end, FISMA establishes clear criteria to improve federal agencies' cybersecurity programs including:

- Periodic risk assessments and risk-based policies and procedures that cost-effectively reduce information security risks to an acceptable level and ensure that information security is addressed throughout the life cycle of each information system
- Comprehensive plans for providing adequate information security for networks, facilities, and systems or groups of information systems
- Security awareness training for agency personnel, including contractors and other users of information systems who support the operations and assets of the agency
- Regular periodic testing and evaluation of the effectiveness of information security policies, procedures and practices
- A process for planning, implementing, evaluating and documenting remedial plans of actions and milestones (POA&Ms)[3] to address any deficiencies in the information security policies, procedures and practices of the agency
- Procedures for detecting, reporting and responding to security incidents
- Plans and procedures to ensure continuity of operations (COOP) for information systems that support the operations and assets of the agency

- Annual reports to the US Office of Management and Budget (OMB), selected congressional committees, and the Comptroller General on the adequacy of information security policies, procedures and practices and on compliance with FISMA's requirements

FISMA is supported by Federal Information Processing Standards (FIPS) 199 and 200 and several NIST SPs (SP 800 series), most of which are evolving to counter the latest cybersecurity threats and to thwart others.

A SEA OF CHANGE IN OVERALL CYBERSECURITY

Effectively dealing with cyberthreats requires looking at and evolving the FISMA "family" both strategically as well as tactically. Strategically, it requires building a consistent, uniform information security framework for the federal government and supporting contractors, which is the overall strategic vision for FISMA, and includes:

- Integrating information security and privacy requirements into enterprise architecture
- Applying systems engineering techniques/approaches to develop more secure information systems

Figure 1 shows the convergence of US federal, civilian, defense and intelligence security approaches into a unified FISMA strategic framework.

Tactically, such unification requires adjusting the FISMA "family" of standards based on cutting-edge best practices and lessons learned.

Tactical actions for cybersecurity readiness include:

- Revising the FISMA legislation to address the latest cybersecurity threats
- Updating the security controls catalog and baselines (NIST SP 800-53 revision 3)
- Updating the certification and accreditation (C&A) process (NIST SP 800-37 revision 1)
- Developing enterprisewide risk management guidance (NIST SP 800-39)
- Providing better guidance on risk assessments (NIST SP 800-30 revision 1)

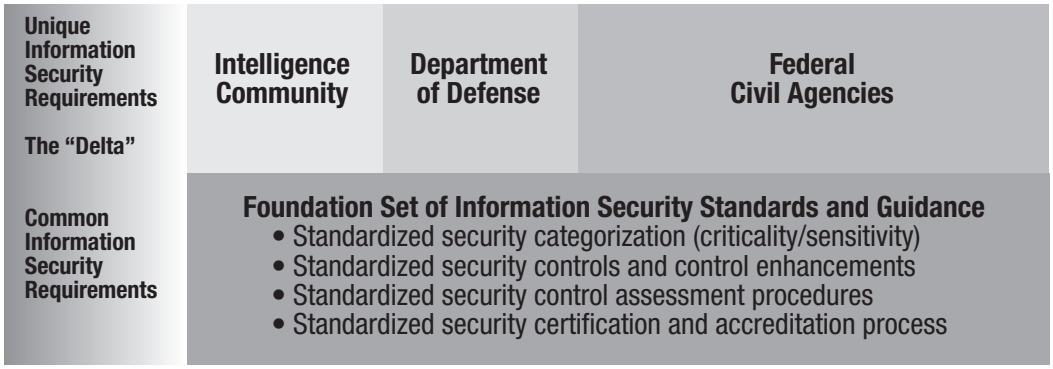
FISMA IS CHANGING

Most security pundits agree that the current implementation of FISMA is inadequate to meet the new challenges posed by cyberthreats. As an example, under current FISMA regulations, agencies must show how they comply with the processes determined to secure IT systems. However, to counteract continuously evolving cyberthreats, FISMA would have to rely less on compliance and more on ways to establish in real time whether systems and networks are truly secure.

Key upcoming FISMA changes include:

- Requiring federal chief information security officers (CISOs) to meet program management, training, governance, oversight, and independent verification and validation (IV&V) challenges
- Modernizing the FISMA platform using CyberScope, which is the new interactive data collection tool, and unlocking the value of reported data by publishing it on a cybersecurity dashboard
- Continuous monitoring of management, operational and technical controls

Figure 1—Convergence of US Federal, Civilian, Defense and Intelligence Security Approaches



- Requiring attack-based and outcome-focused metrics, making agencies demonstrate that their systems are effectively protected against known vulnerabilities, attacks and exploitations
- Focusing on situational awareness to move toward real-time security

All of these changes are aimed at recognizing the interconnected nature of the Internet and agency networks; improving the situational awareness of government cyberspace; enhancing information security of the US federal government; unifying policies, procedures and guidelines for securing information systems and national security systems; and establishing security standards for government-purchased products and services.

The bottom line is that the focus of cybersecurity is shifting from compliance to risk-based protection.

NEW SECURITY CONTROL GUIDANCE WITH NIST 800-53 REVISION 3

Recommended Security Controls for Federal Information Systems and Organizations, also known as NIST SP 800-53, provides guidelines for selecting and specifying security controls for information systems that support the executive agencies of the federal government to meet the requirements of FIPS 200, *Minimum Security Requirements for Federal Information and Information Systems*. The guidelines in this special publication are applicable to all federal information systems except those systems designated as national security systems. Revision 3 introduces many changes to its predecessor, including:

- Lessons learned from the Interagency Assessment case project. Its goal was to provide a multiagency recommendation for the specific actions an assessor may perform in applying the assessment procedures in NIST SP 800-53A.
- Security controls for civilian, defense and intelligence systems
- Best practices in information security from the US Department of Defense, the intelligence community and civil agencies
- Material from the Committee on National Security Systems (CNSS) instruction 1253[4] (as part of the unification)
- New security controls to address cyberthreats
- Plans for incorporating a threat appendix for cyberpreparedness

A new concept of priority codes has been introduced to assist in making sequencing decisions for control implementation. Additionally, a new management and common control concept is outlined with the introduction of the organizationwide information security program plan. Another exciting addition is the strategy for harmonizing FISMA security standards and guidelines with the international information security management standard ISO/IEC 27001, *Information technology—Security techniques—Information security management systems—Requirements*.

It would be naive to assume that so many changes would not have a noticeable impact on the application of the publication in practice. Major modifications will be required to existing system security documentation to incorporate the baseline control variances. For example, existing system security plans, contingency plans and documentation templates will have to incorporate new security controls and enhancements.

NEW C&A GUIDELINES WITH NIST 800-37 REVISION 1

Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach, NIST SP 800-37, provides guidelines for the security authorization of federal information systems. This publication has also undergone considerable revision with four key goals in mind:

1. Develop a common security authorization process for federal information systems (currently known as the C&A process).
2. Make the risk management framework and accreditation process an integral part of the system development life cycle (SDLC).
3. Provide a well-defined and comprehensive security authorization process that ensures responsibility and accountability for managing information system-related security risks.
4. Incorporate a risk executive function into the security authorization process to ensure that decisions are based on an "enterprise" view of risk and that they consider all factors, including mission, IT, budget and security.

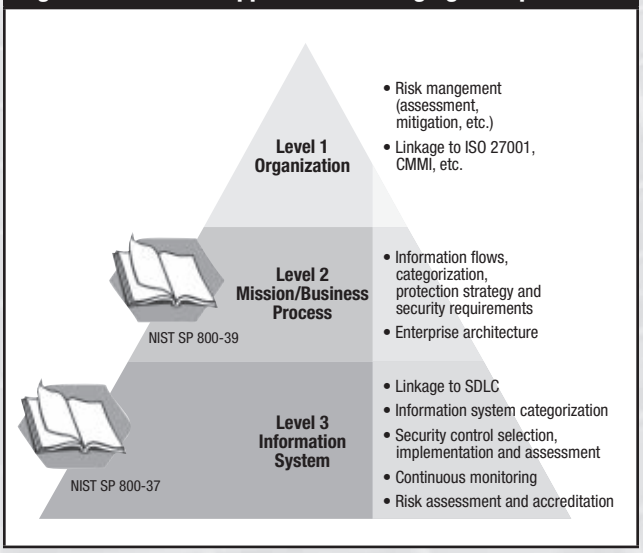
There is a special emphasis on continuous monitoring via automated support tools and ongoing security authorizations.

NIST 800-39: MANAGING RISK AT AN ENTERPRISE LEVEL

Risk management is a central theme in all of the revisions that this article has covered thus far. To that end, the entire risk management framework is being reworked to shift focus from managing risk at the information systems level to the enterprise level. The development of SP 800-39 is the first step in this two-step redesign process. Step two is revising the current NIST recommendation on risk management, NIST SP 800-30, to focus exclusively on risk assessment as it applies to the various steps in the Risk Management Framework (RMF) described in SP 800-39. Truly, SP 800-39 stands out as a flagship document in the series of FISMA-related publications by providing a risk management framework that allows a structured yet flexible approach for managing the risk resulting from using information systems.

The complexity and diversity of mission/business processes in modern organizations and the multitude of information systems that are needed to support those processes require a holistic approach to building effective information security programs and managing organizational risks. Managing risk with an enterprise perspective requires looking at risk in a "tiered" manner, as shown in **figure 2**. **Figure 2** also shows where SPs 800-37 and 800-39 fit with respect to risk management. Managing organizational risk (level 1) is beyond the scope of current NIST SPs.

Figure 2—A Tiered Approach to Managing Enterprise Risk



Risk management is a six-step process, as illustrated in **figure 3**. These six steps are paramount to effective organizationwide management of risk resulting from the operation and use of information systems:

1. Categorize the information and systems (impact/criticality/sensitivity).
2. Select and tailor the security controls. This includes tailoring and supplementing the security controls based on the risk assessment.
3. Implement and document the security controls in the information system.
4. Assess the security controls for effectiveness.
5. Decide the enterprise/agency-level risk and risk acceptability, and authorize information systems operation.
6. Monitor security controls on a continuous basis.

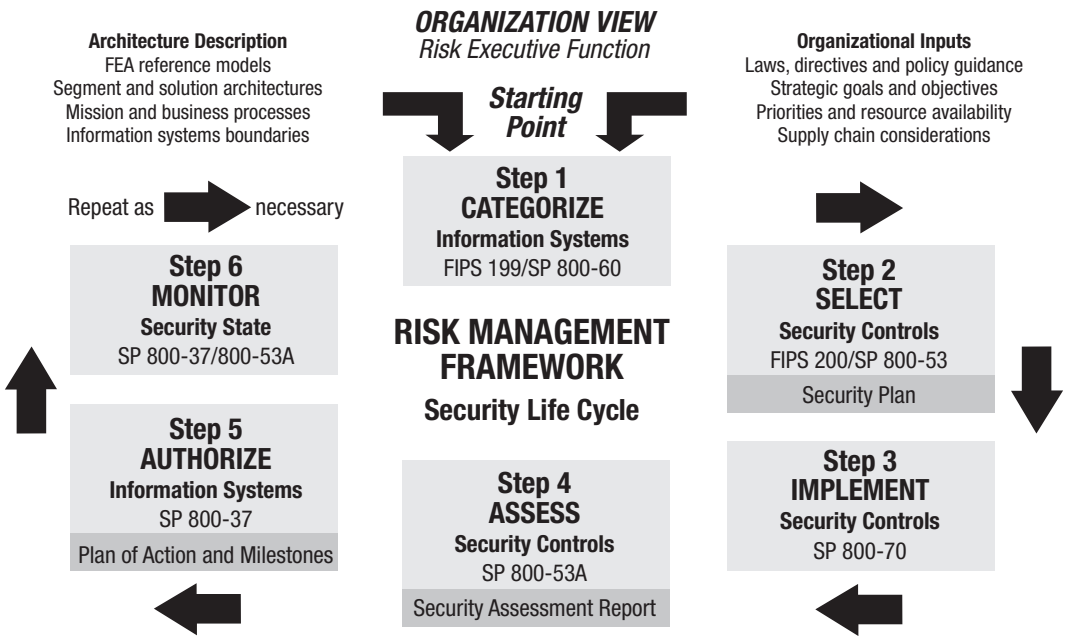
SP 800-39 introduces the concept of a risk executive function with the overall goal of ensuring that information security considerations and authorization decisions for individual information systems are viewed from an organizationwide perspective with regard to the overall strategic goals and objectives of the organization in carrying out its mission/business processes. **Figure 4** depicts this process.

SP 800-39 also reemphasizes the importance of continuous monitoring of risk by stating that:

> *…Conducting thorough point-in-time assessments of security controls in organizational information systems and supporting infrastructure is a necessary but not a sufficient condition to demonstrate security due diligence and to manage risk. Effective information security program should also include comprehensive continuous monitoring programs to maintain on-going, up-to-date knowledge by senior leaders of the organization's security state and risk posture and to initiate appropriate responses as needed when changes occur.*[5]

Continuous monitoring programs are an important step toward ensuring that the implemented security controls continue to be effective over time as changes within the system or the operating environment occur. Continuous monitoring also ensures that when existing controls are deemed to be ineffective at satisfying the security requirements, the necessary steps of the RMF are engaged

Figure 3—The Risk Management Framework



to systematically address adjustments in the controls. Thus, a well-designed and well-managed continuous monitoring program can effectively transform an otherwise static security control assessment and risk determination process into a dynamic process that provides near real-time security status information to the appropriate agency officials.

CONCLUSION

FISMA and the supporting NIST publications are changing to incorporate lessons learned, to counter new and evolving cyberthreats, and to manage enterprise risk using an integrated SDLC approach. These changes are aimed at preventing exploitation of security vulnerabilities, unauthorized access, and loss of sensitive data or personally identifiable information (PII) and, ultimately, at obtaining funding for current and future projects. With so much at stake, is it any wonder that the only option is getting ahead of the game?

REFERENCES

1105 Government Information Group, "Agencies Report 200% Increase in Cybersecurity Attacks," *FederalDaily.com*, 21 July 2009, *www.federaldaily.com/federaldaily/archive/2009/07/FD072109.htm*

CISCO, Government Futures and (ISC)², *The 2009 State of Cybersecurity From the Federal CISO's Perspective—An (ISC)²® Report*, USA, 2009, *http://media.haymarketmedia.com/Documents/7/FederalCISOSurveyReport_1638.pdf*

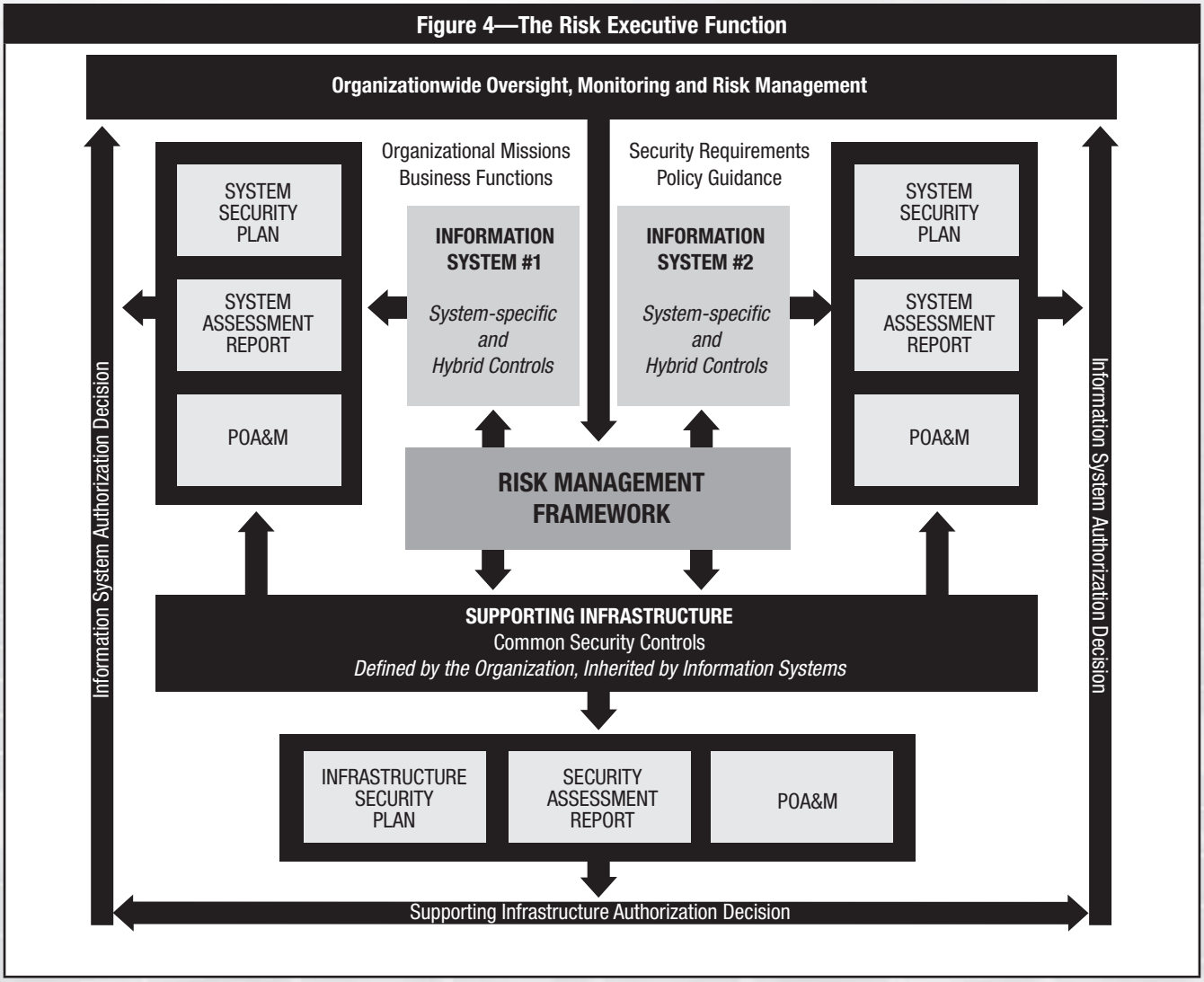
NIST, *Risk Management Guide for Information Technology Systems*, SP 800-30, USA, 2002, *http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf*

NIST, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach, SP 800-37, Revision 1*, USA, 2010, *http://csrc.nist.gov/publications/nistpubs/800-37-rev1/sp800-37-rev1-final.pdf*

NIST, *Recommended Security Controls for Federal Information Systems and Organizations, SP 800-53 Revision 3*, USA, 2009, *http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final_updated-errata_05-01-2010.pdf*

National Science and Technology Council, *Federal Plan for Cyber Security and Information Assurance Research and Development*, USA, April 2006, *www.itrd.gov/pubs/csia/csia_federal_plan.pdf*

Figure 4—The Risk Executive Function



ENDNOTES

[1] GAO, *Agencies Continue to Report Progress, But Need to Mitigate Persistent Weaknesses*, GAO Report to Congress, USA, July 2009, *www.gao.gov/new.items/d09546.pdf*

[2] GAO, *Emerging Cybersecurity Issues Threaten Federal Information Systems*, GAO Report to Congress, USA, May 2005, *www.au.af.mil/au/awc/awcgate/gao/d05231.pdf*

[3] Per the "Memorandum for the Heads of Executive Departments and Agencies" issued by the White House, a POA&M is a tool that identifies tasks that need to be accomplished. It details resources required to accomplish the elements of the plan, any milestones in meeting the task and scheduled completion dates for the milestones. The purpose of this POA&M is to assist federal agencies in identifying, assessing, prioritizing and monitoring the progress of corrective efforts for security weaknesses found in programs and systems. USA, 2001, *www.whitehouse.gov/omb/memoranda_m02-01/*

[4] CNSS Instruction No. 1253, USA, October 2009, *http://www.cnss.gov/Assets/pdf/CNSSI-1253.pdf*

[5] NIST, *DRAFT Managing Risk From Information Systems: An Organizational Perspective*, SP 800-39, USA, 2008, *http://csrc.nist.gov/publications/drafts/800-39/SP800-39-spd-sz.pdf*

Giving Sustainability to COBIT PO9

Vítor Prisca, CISM, CGEIT, is an executive director at Novabase and the principal of the IT management practice. He assisted in the expert review of COBIT 4.0 and is a certified consultant for International Organization for Standardization (ISO) 20000 and 27001. Prisca also delivers training in IT best practices, compliance (US Sarbanes-Oxley Act and Basel II), business continuity and information security management.

Manuel Moreira, CISA, IPMA Level C: Certified Project Manager, is a manager at Novabase. He has vast experience with customer projects in the areas of compliance, internal control, process design and implementation, security, and audit.

This article presents an effective methodological approach to implement and sustain the COBIT PO9 *Assess and manage IT risks* process. This process belongs to the Plan and Organize domain of the COBIT framework and is key for any organization concerned with managing and controlling its risks. It is a core process for any internal control framework that must comply with laws and regulations such as the US Sarbanes-Oxley Act or Basel II. Although this strategy was applied to this process only, in a large international financial group (€100 billion), this approach may be applicable to other processes of the COBIT framework, with significant advantages in terms of rightsizing the implementation project.

GIVING SUSTAINABILITY TO PO9

Obtaining a high level of maturity for the PO9 process is apparently a trivial task. The experience in this case[1] shows that a management system can be put in place in three to four months. But, because PO9 requires a context to be fully operational, a methodology is required to identify a manageable set of assets and activities in which risk management can be applied, producing visible results in a reasonable time frame and with a justifiable amount of resources.

The approach described in this article is based on COBIT 4.1 and is independent from the context in which risk management occurs.

DESCRIPTION OF THE CONTEXT

Operational risk management has become mandatory for many institutions because there are external drivers such as Basel II and other international and country-specific regulatory requirements. Valorization of risk, as a decision tool for the choice of controls that protect the organization's assets, is sufficient justification for operational risk to encompass IT practices and IT operations. IT organizations now believe that addressing risk is no longer a matter of choice; it is a requirement from both a financial and compliance point of view.

This is not the only motivation. Project management standards and best practices have risk management requirements in common. Another strong motivation is the need to keep the costs of controls at a reasonable level. Risk assessment and evaluation provide the necessary inputs to reduce the risks to acceptable levels while investing the "right" amount of money. Stakeholders also fear for their investments and require reasonable assurance that risks are managed in a proficient manner by management.

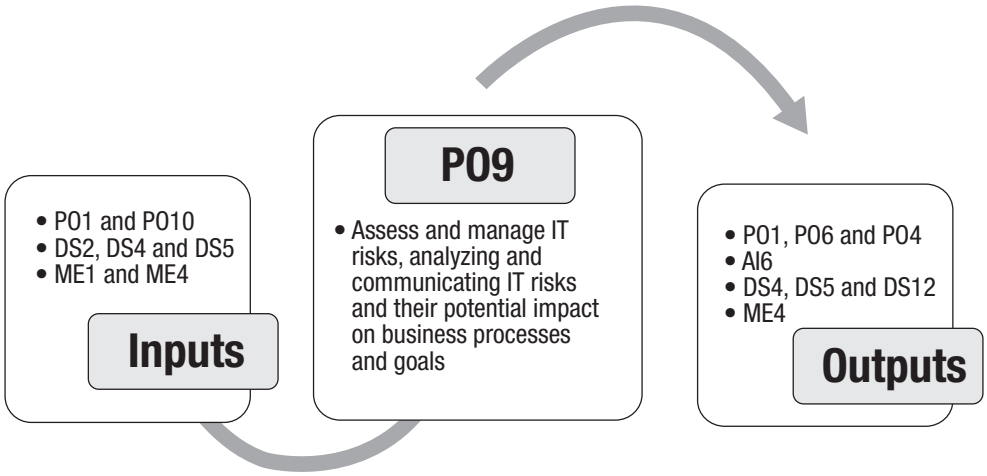
The case described in this article occurred in a company that is the only supplier of IT services to a large international financial institution. The boards of both companies were fully aligned with the need to have a systematic approach to risk management, and the initiative took place with their full sponsorship.

The objective of the project was to implement the recommendations of ISO 31000, *Risk management*, ensuring at the end a maturity level of at least three for PO9. The set of deliverables included a risk management policy; risk management processes; a description of functions; a context manual; a list of threats, vulnerabilities and risks; a baseline of key performance indicators (KPIs) and key risk indicators (KRIs); a risk assessment tool; and training materials. These deliverables are just the foundation for what an organization needs to do. Additional actions are required to achieve a continual and sustainable attitude toward risk.

THE CHALLENGE

Basel II and other local regulations issued by the Bank of Portugal are now in effect, and as a result, it is in the best interest of financial institutions to implement a sound operational risk management system in the shortest period of time without compromising compliance with the various requirements. The obvious place to start was to define the policies and processes required by the organization. This approach, although sound, is a lengthy one and has a prerequisite: a

Figure 1—PO9 Relationship Diagram



careful choice of processes. Another very lengthy path, while absolutely and formally correct, is to make an inventory of the organization's assets and perform a thorough risk assessment cycle.

The challenge in this project was to choose a strategy that could provide quick wins, that was supported by a good rationale and fully coherent with the recently adopted risk management methodology, and that was sound enough to be accepted by internal audit and the regulator.

THE METHODOLOGY

The internal control system of the IT organization was being built using COBIT as the main source of good control practices. Consequently, the design of the rationale and the strategy had to be supported by COBIT also.

COBIT 4.1's framework, control objectives, management guidelines and maturity models indicate, for each process, the required input and output processes. It can be established that every process needs to be implemented in an enabling and supporting environment, with the objective to increase process maturity levels and, thus, control effectiveness. To achieve its goals, a process needs activities and information provided by external sources. Each goal can be better achieved when each activity is executed properly and when data are available and reliable.

As such, there was a need to ensure that the PO9 process was receiving the required inputs from other processes, even if those processes were not yet in place or, because of reduced maturity or lack of implementation scope, they were not delivering the expected outputs.

PO9 *Assess and manage IT risks* is framed by processes as shown in **figure 1**.

Figure 2 shows the minimum requirements to set up the PO9 process. COBIT's management guidelines provide a fairly comprehensive description of the required inputs. Following these guidelines throughout the design phase of the risk management processes provided a foundation for a reliable and comprehensive strategy to ensure a consistent, "clean and lean" approach to PO9's design, implementation and sustainability and, thus, to ensure a management-optimized methodological approach.

Figure 2—PO9 Management Guidelines

From	Inputs
PO1	Strategic and tactical IT plans, IT service portfolio
PO10	Project risk management plan
DS2	Supplier risks
DS4	Contingency test results
DS5	Security threats and vulnerabilities
ME1	Historical risk trends and events
ME4	Enterprise appetite for IT risks

Source: IT Governance Institute, COBIT 4.1, USA, 2007

Having identified the processes, the second step was to look again at COBIT and clearly identify which inputs PO9 was expecting from the processes included in the relationship diagram. Each of the mentioned processes produced a specific output that had to be fed into the PO9 stream of operational processes (those that the organization recognizes and executes

on a daily basis). Many other assets had to be run through risk management. The management guidelines (**figure 2**) contain the minimum requirements for any organization. In fact, the main goal of implementing PO9 is to ensure that the organization's assets have an adequate level of protection against threats that explore the existing vulnerabilities.

Analyzing the list of inputs, it became obvious that COBIT suggests that an organization should look first to the following assets:

- The services provided by the IT organization to the business
- The components of the infrastructure that support the services
- The projects
- The suppliers' services
- The continuity plans

Then, the organization should build the list of threats and vulnerabilities that are applicable to its assets.

Risk analysis is more efficient when supported by historical data. This is referred to as historical risk trends and events. In the absence of historical data, a qualitative approach should be developed based on personal experience, technical expertise and the data provided by manufacturers and suppliers.

Having identified the inputs for PO9, the next challenge was to identify where and how they were produced. Fully documented operational processes and management are normally the first sources of information. When this is not the case, the task is more efficient when supported by a typical map of functions that are normally responsible for producing such inputs.

Again, COBIT is a reliable source of planning information. The Responsible, Accountable, Consulted and Informed (RACI) charts indicate who in the organization is responsible for the production of each input. The results of using the RACI tables for PO1, PO10, DS2, DS4, DS5, ME1 and ME4; selecting the proper activities; and then choosing just the responsible functions are shown in **figure 3**.

Using the information in **figure 2**, gathered using the management guidelines, a solid reference was built and can be used to understand where the relevant functions are located in the organization chart and whether their responsibilities involve the production of the required inputs.

COLLECTING THE EVIDENCE

The next objective was to understand how many inputs exist, how effective and how mature the production process is, if there are any threats associated with the process, which controls are in place to ensure that risks are being managed, and also which process controls exist.

The evidence that is collected has to be recorded exactly as when a self-assessment is being performed. It is not relevant at this point to analyze the content of the inputs in great detail. That is the job of the PO9 process.

PROCESSING THE RESULTS

A self-assessment or an independent audit reveals if the inputs exist and, if they exist, what their maturity level is. It is at this point that usage of PO9 becomes operationally relevant.

PO9 control objectives are clear. The organization needs a framework, a clear context, and processes designed and in operation regarding the event identification, the assessment of risk and the response to risk.

The first question to ask: Is there any way in which the inputs are related to the organization's risk assessment context? In short, the risk assessment context is a document that describes, among other things, the assets that are relevant to the organization, the risk assessment criteria and the threat baseline.

The information collected, or the lack of it, should drive a KRI evaluation. COBIT control practices provide information to create a list of KRIs. They can be derived from the risk drivers and complemented by the risk appetite defined by management. The values obtained provide direction to the amount of remediation required to lower the level of risk to which the organization is exposed.

THE RISK IT FRAMEWORK

The previously mentioned risk management project took place during 2008. The Risk IT framework had not been published yet. All the project work was based on a working draft of ISO 31000 and, of course, the PO9 control objectives and control practices.

Published in 2009, Risk IT has a comprehensive process model[2] that could be useful to achieve the objectives described in this article.

Figure 3—PO9 Functions Perimeter Table

Process	Activity	Outputs	Board	CEO	CFO	Business Executive	CIO	Business Process Owner	Head Operations	Chief Architect	Head Development	Head IT Administration	PMO	Compliance, Audit, Risk and Security
PO1	Build an IT strategic plan.	Strategic plan		A	C	C	R	I	C	C	C	C	I	C
	Build IT tactical plans.	Tactical plan		C	I		A	C	C	C	C	C	R	I
	Analyze program portfolios and manage project and service portfolios.	IT service portfolio		C	I	I	A	R	R	C	R	C	C	I
PO10	Build project charters, schedules, quality plans, budgets, and communication and risk management plans.	Project risk management plan				C	C	C	C	C	C	C	A/R	C
DS2	Identify, assess and mitigate supplier risks.	Supplier risks			I		A		R		R	R	C	C
DS4	Regularly test the IT continuity plan.	Contingency test results					I	I	A/R		C	C	I	I
DS5	Conduct regular vulnerability assessments.	Security threats and vulnerabilities			I		A	I	C	C	C			R
ME1	Identify and collect measurable objectives that support the business objectives.	Historical risk trends and events		C	C	C	A	R	R		R			
ME4	Review, endorse, align and communicate IT performance, IT strategy, and resource and risk management with business strategy.	Enterprise appetite for IT risks	A	R	I	R								C

Process goals RG1, RG2 and RG3, all three linked to Risk Governance (RG), supply the necessary guidance to define the context in which risk management occurs in a particular institution.

Define IT risk analysis scope, a key activity of process goal RE3, helps to identify the relevant assets for analysis. RE3 brings attention to collecting historical data that are later needed for the estimation of IT risk (RE2.2).

CONCLUSIONS

COBIT can be used beyond control objectives. This simple example shows one of the benefits that COBIT's management guidelines can bring when a decision has to be made about the scope of applicability of a particular process—in this case, PO9.

This example could become more complex just by adding additional input processes to the set of processes that have been mentioned. The increase in complexity is due to the amount of information that has to be treated, but not to the methodology itself. ISACA provides a good source for financial institutions to identify the additional projects: *IT Control Objectives for Basel II.* This book provides a sound rationale for the list of COBIT processes in scope.

While COBIT sets good practices for the means of risk management by providing a set of controls to mitigate IT risk, Risk IT sets good practices for the ends by providing a framework for enterprises to identify, govern and manage IT risk.

ENDNOTES

[1] This is based on the authors' recent experiences with COBIT and PO9 in particular.

[2] ISACA, *The Risk IT Framework*, USA, 2009, *www.isaca.org/riskit*

Use of the Balanced Scorecard for IT Risk Management

Rajesh Kapur, CISA, FIETE, MIE, is a director at Tyche IT Consultants. He has been a professor of computer science and engineering at BIET, Hyderabad, India; and a faculty member at the Institute of Chartered Financial Analysts of India (ICFAI) Business School, Hyderabad, India. Kapur has been a senior project manager at Synfosys Business Solutions, deputy general manager at the Corporate IT Division of Apollo Hospitals, and director (solutions) at winAMR Systems. He can be contacted at *kapursam@rediffmail.com.*

Risk management, in its essence, is subjective. Though it is a structured approach to determine whether to accept, mitigate, transfer or avoid a risk, it is based on a subjective assessment of the business impact of the exercise on organizational vulnerability. The current slowdown in business profitability has brought into greater focus the need for risk management initiatives to quickly align with the business goals of an enterprise. Business goals will change from time to time, as will the perception of their associated vulnerabilities and their consequent impact. The process of risk management must be in line with this change. In a dynamic business environment necessitating change in business goals and objectives, the "in line" aspect of risk management (with business goals) percolates down to the management of risks associated with the optimal deployment of IT resources.

THE BALANCED SCORECARD

There are numerous factors that impact the business goals and objectives of an enterprise and, thereby, contribute to the need for change. The change may be driven by market forces or may be a result of an internal shift in priorities. These factors, varied and divergent as they are, can be effectively abstracted by means of a balanced scorecard (BSC) approach.

The BSC approach has evolved from its early use as a simple performance measurement framework to a full-fledged strategic planning and management system. It is used across all sectors of business and industry to align enterprises' business activities to the vision and mission of the organization, to improve internal functioning and customer perception of an organization, and to monitor the organization's performance against strategic goals. It spawns a framework for performance metrics and delineates objectives, from which management can execute strategies. BSC has the potential to oversee the mechanism of converting a long-term strategic plan into sets of immediately doable activities.

Although a great deal of literature is available on the BSC, it is abstracted for the purposes of this article in **figure 1**. Each of the four perspectives is briefly elucidated as follows:

- The financial perspective is focused on ensuring that the execution of the strategy of an enterprise is contributing to bottom-line growth. Revenue growth, costs, profit margins, cash flow and net operating income are some illustrative metrics that are incorporated into the planning and evaluation of an enterprise's activities *vis-a-vis* this perspective.
- The customer perspective is focused on the value proposition (based on the appropriate mix of operational excellence, customer relationship management and product share) that the enterprise implements to generate greater sales by courting its customers.
- The internal business processes perspective focuses on the processes that create and deliver the product's value proposition for the customer. Included in these processes are those that deal with (but are not limited by) operations, regulation, compliance, innovation, and the discharge of social and corporate responsibility.
- The learning and growth perspective focuses on the foundation of any strategy: the intangible assets of an organization, which primarily comprise the internal skills and capabilities that are required to mentor and support the value-creating internal processes. Though investment in these assets usually decreases the short-term bottom line, it is necessary to realize long-term goals and success of an enterprise.

Figure 1—BSC Model

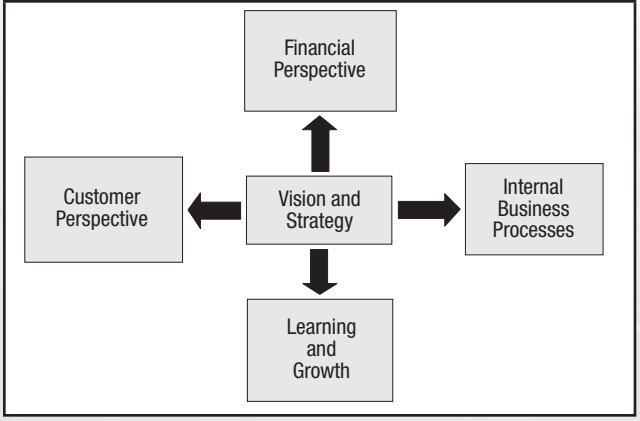
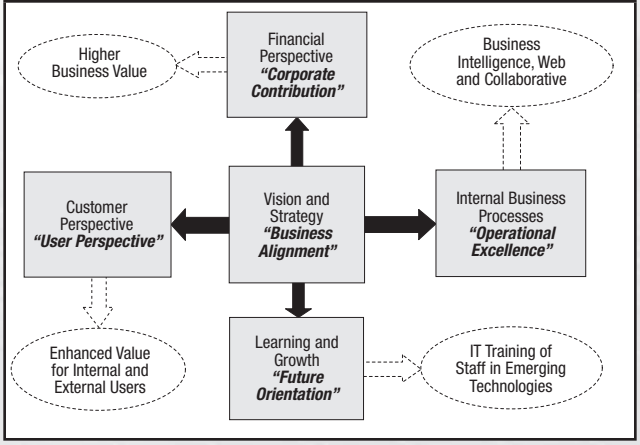


Figure 2—Corporate BSC Mapped to IT BSC



MAPPING TO AN IT SCORECARD

The BSC methodology can provide a measurement and management system that supports the process of IT governance as well as the more critical aspect of alignment of IT governance to corporate goals and objectives.[1] Under this proposal, an IT BSC links with business through the business contribution perspective—by explicitly expressing the relationship between IT and business via a mapping of business goals and objectives to IT goals and objectives. The IT BSC, after mapping the various perspectives, is shown in **figure 2** (the mapped IT perspectives are shown in bold italics).

The mapping is a tool used to provide direction on how to impart maximum value for the organization through technology. It traces the consequential relationship between strategic goals determined by the corporate BSC and the consequent strategic objectives as relevant to the IT domain of an IT BSC (the respective objectives are within ovals in **figure 2**). For example, improving performance in the objectives found in future orientation (learning and growth) enables the organization to improve its operational excellence (internal business processes), which in turn enables the organization to create desirable results in the customer and financial perspectives. There is a cause-and-effect relationship here that plays out as the enterprise moves through various stages of its life cycle.

IT departments can control risk by developing and deploying application controls to ensure completeness, accuracy, validity, authorization and segregation of duties, but accruing business value through risk management will require an understanding of the current priorities of the enterprise—in effect, those of senior management. These would be guided not only by various social, economic and environmental factors, but also by the specific stage of the life cycle of the enterprise.

Risk management, subjective as it may be, has to be an inherent aspect of any successful business effort; it is carried out either explicitly or implicitly at both the operational and strategic levels of an enterprise. It is an essential constituent of sound corporate governance. Just as the IT BSC can be deduced from the corporate BSC to better align itself with corporate business objectives, a methodology for technology risk management can be deduced from the corporate BSC to facilitate effective IT risk management.

This article aims at extrapolating the technique of using the BSC for IT governance to the task of IT risk management for an enterprise. It factors in the cause-and-effect relationship elucidated previously. Deployment of the methodology will enhance the level of sensitization of the technology risk management process to its most critical requirement—alignment with corporate goals and objectives.

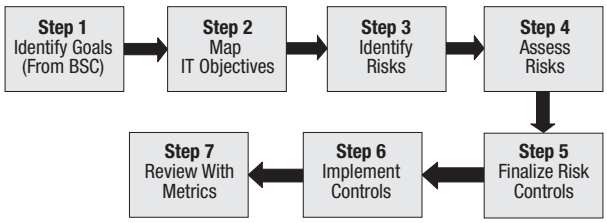
THE METHODOLOGY

The methodology includes the following seven steps (see **figure 3**):

- **Step 1:** Identify the current set of BSC goals. This activity is carried out at the highest levels of the organization. The chief information officer (CIO) must keep abreast of the goals and must ensure that any noticeable shift in priorities is (implicitly or explicitly) detected and expeditiously translated into an IT risk management plan.

- **Step 2:** Map the current set of BSC goals to actionable technology objectives, and establish the context in which the risk assessment framework is applied to ensure appropriate outcomes. This should include the objective of the assessment to a BSC goal, including delineating the context of each risk assessment against the business criteria sought to be achieved.
- **Step 3:** Develop a risk identification system based mainly on the objectives determined in step 2. The main activities to be carried out at this stage are the profiling of specific threats and vulnerabilities to the attainment of the objectives.
- **Step 4:** Carry out a risk assessment, taking into account the probability of occurrence, business impact (of the occurrence of vulnerability) and prioritization as per the standard methodology. Information security and compliance are not the only issues here. Threats to competitive advantage, reputation, furthering the mission, etc., have to be considered. Only by a holistic consideration of the entire spectrum of an organization's activities and due prioritization is a technology risk assessment finalized.
- **Step 5:** Determine the specific risk control strategy as a combination of one or more of the following, in respect of each risk assessed:
  - Risk avoidance
  - Risk transfer
  - Risk mitigation
  - Risk acceptance
- **Step 6:** Implement the system as per the system development life cycle (SDLC) methodology, with the enumerated strategy as an integral part of the requirement and analysis phases. This is the stage at which a risk response process should be developed and maintained. It should be designed to ensure that cost-effective controls align themselves with the specific risk control strategy chosen on a continual basis. Provisions for making allowance for risk management due to compliance and regulatory guidelines would be in addition to the risk management efforts deduced from the BSC.
- **Step 7:** Periodically review whether the technique is proving effective. The associated metrics will have to be identified at the initial stages. The final assessment must also be modulated by the subjectivity inherent in all risk-related activities. Some suggested metrics are:
  - The percentage of risk management effort that is earmarked, as a result of BSC priorities, as a part of the overall risk management effort. It is suggested that this should not be less than 60 percent.
  - The percentage of actual critical events that have impacted business as a part of those envisaged during the risk assessment stage
  - Number of significant incidents caused by risks not identified in the risk management process, as well as their respective business impact
  - Frequency of review of the technology risk management process
  - Cost-benefit analysis of the implementation of the controls

Figure 3—IT Governance BSC Methodology



CRITICAL SUCCESS FACTORS

Risk management has now become inherent in all corporate endeavors. Getting all the stakeholders to focus on true essentials remains a challenge. Critical success factors (CSFs) help in delineating the essential areas of activity that must be performed well to achieve business goals.

The CSFs for technology risk management through the use of the BSC are as follows:

- The priorities as set by the BSC must be unambiguous and based on technology abstractions by the CIO (function) that have been mapped from facts sourced from:
  - Business intelligence and data
  - Stakeholder expectations
- The mapping from technology abstractions to discrete IT objectives must be parameterized, and thresholds must be set for each parameter. In the absence of past data, approximation and estimation techniques should be employed.
- The risk assessment must always make allowances for performance, scale, security and disaster, apart from the objectives set by the BSC.

- Change management must be effective whenever there is a shift in corporate priorities. This includes:
  - Identifying the drivers of the change and their respective responsibilities (i.e., who will do what)
  - Establishing a road map for change along with the milestones
  - Ensuring that monitoring and controls are in place on a periodic basis

CONCLUSION

At the end of the risk management activity, there is always a question that the stakeholders would like to have answered with a fair amount of certainty: "Have we got it right?"

The question can be answered to any acceptable amount of precision only by constant observation and review—by being proactive rather than reactive.

Success in any technology risk management activity, however, relies heavily on the commitment shown by senior management; the competence of the risk assessment team to translate business requirements into IT objectives; the support and participation of the IT team; and the awareness, cooperation and support of all employees in the organization who must comply with the controls to make the vision of their organization a reality.

REFERENCES

Fischer, Urs; "Identify, Govern and Manage IT Risk Part 1: Risk IT Based on CobiT Objectives and Principles," *ISACA Journal*, vol. 4, 2009

Schlarman, Steve; "IT Risk Exploration: The IT Risk Management Taxonomy and Evolution," *ISACA Journal*, vol. 3, 2009

Nash, Kim S.; "Armed for Safety," *Real CIO World*, vol. 4, issue 5, 15 January 2009

Ross, Steven; "Dumb Luck," *ISACA Journal*, vol. 1, 2008

Buchler, Kevin; Andrew Freeman; Ron Hulme; "The New Arsenal of Risk Management," *Harvard Business Review South Asia*, September 2008

Stoneberner G.; *et al*; "Risk Management Guide for Information Technology Systems," Special Publication, 800-30, National Institute of Standards and Technology (NIST), July 2002

ENDNOTES

[1] Van Grembergen, W.; "The Balanced Scorecard and IT Governance," *Information Systems Control Journal*, vol. 2, 2000

EDITOR'S NOTE

Collaborate with ISACA members and access additional resources on this topic in the ISACA Knowledge Center located at *www.isaca.org/knowledgecenter*.

Prepare for the **2010** CISA Exams

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

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

www.isaca.org/elearning

www.isaca.org/cisareview

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

CISA Review Manual 2010

ISACA

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

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

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

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

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

The 2010 edition has been developed and is organized to assist candidates in understanding essential concepts and studying the following job practice areas:
- IS audit process
- IT governance
- Systems and infrastructure life cycle management
- IT service delivery and support
- Protection of information assets
- Business continuity and disaster recovery

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

CISA Review Questions, Answers & Explanations Manual 2010

ISACA

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

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

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

CISA Review Questions, Answers & Explanations Manual 2010 Supplement

ISACA

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

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

CISA Practice Question Database v10

ISACA

The CISA® Practice Question Database v10 combines the *CISA Review Questions, Answers & Explanations Manual 2010* with the *CISA Review Questions, Answers & Explanations Manual 2010 Supplement* into one comprehensive 900-question study guide. Sample exams with randomly selected questions can be taken and the results viewed by job practice, allowing for concentrated study one area at a time. Additionally, questions generated during a study session are sorted based upon previous scoring history, allowing CISA candidates to easily and quickly identify their strengths and weaknesses and focus their study efforts accordingly. Other features provide the ability to select sample exams by specific job practice areas, view questions that were previously answered incorrectly and vary the length of study sessions. The database software is available in CD-ROM format or as a download.

PLEASE NOTE the following system requirements:
- 400 MHz Pentium processor or equivalent (minimum); 1 GHz Pentium processor or equivalent (recommended)
- Supported operating systems: Windows Server 2003, Windows Server 2008, Windows Vista, Windows XP
- 512 MB RAM or higher
- One hard drive with 250 MB of available space (flash/thumb drives not supported)
- Mouse
- CD-ROM drive

CDB-10 English Edition—CD-ROM
CDB-10W English Edition—Download
CDB-10S Spanish Edition—CD-ROM
CDB-10SW Spanish Edition—Download

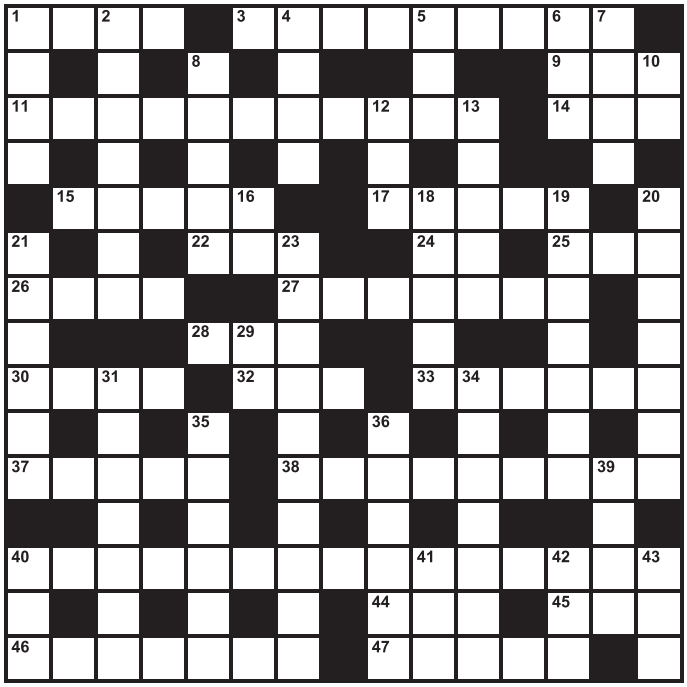
CISA Online Review Course

ISACA

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

Crossword Puzzle

By Myles Mellor
www.themecrosswords.com



ACROSS
1. Head of information security
3. Security software
9. Bottom line
11. Key position in evaluating security dangers and the budget and the need to handle them (2 words)
14. Auction offering
15. Deserve
17. Divide (2 words)
22. Keyboard key
24. ___ plus ultra
25. Audience
26. Keep something hidden, ____ up
27. ____ threat: one of the highest concerns of corporate IT and risk management, especially when downsizing is occurring
28. International organization of standards
30. Inadvisable action (2 words)
32. Monetary fund, abbr.
33. Diagram
37. Minimum number of characters considered to be needed in an effective password
38. Physical security equipment (2 words)
40. Those with access permission (2 words)
44. Meet, of a board
45. Agent
46. Plans
47. ____ phishing: enticing executives to click on links that will download malware or Trojans onto their computers

DOWN
1. Carnegie Mellon group, for short
2. Groups of independent but interrelated elements that comprise a unified whole
4. Minigolf course hole number
5. Compete
6. Web site address
7. Directly
8. Scope
10. Technology department
12. Governance, risk management and compliance, abbr.
13. Evaluated as to quality
16. Teacher's assistant, for short
18. An assemblage of parts that is regarded as a single entity
19. Annually (2 words)
20. Type of malware
21. Modification that has to be documented
23. Form of identity access management
29. Modern form of the metric system, abbr.
31. Nullifies
34. Make a mathematical calculation
35. Effective, as a password
36. The operation of reading or writing stored information
39. Land area
40. Throw in
41. Downturn
42. Slip
43. Secretly collect sensitive or classified information

(Answers on page 54)

HelpSource Q&A

We invite you to send your information systems audit, control and security questions to:
HelpSource Q&A
bgansub@yahoo.com or
publication@isaca.org

Fax to: +1.847.253.1443
Or mail to:
ISACA Journal
3701 Algonquin Road, Suite 1010
Rolling Meadows, IL 60008 USA

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

Q I read your previous column with a question based on the book *8 Things We Hate About IT: How to Move Beyond the Frustrations to Form a New Partnership with IT*. In your response, you discussed 'things we hate about information security'; it made a lot of sense and was interesting reading, too. Continuing the discussion along the same lines, can you please list out the things that people 'hate' about information systems auditors? Auditors do not necessarily, on all occasions, remain best friends with the people in the business/IT. Please also add what auditors must do to win friends.

A I do not disagree with you—auditors who do a clinical, dispassionate job may win the wrath and displeasure of those in the field and, on some odd occasions, even from leadership of the operational area that gets audited. But that does not mean they are 'hated'. Hatred can exist when auditors disappoint and fail to do their job. Not being popular can be misconstrued for hatred, but in the long run, good auditors are not necessarily popular *per se*. The truth of the matter is that by being clinical and dispassionate, with no personal agenda, auditors serve the best interests of their employers and their profession. Here are some areas that can result in auditors being 'hated':

- Auditors who do not choose the right areas for conducting the audits easily earn the displeasure of both operational and organisational leadership. Unless the right domains or organisation units get audited, it will be a waste of resources, both from the audit perspective and from that of the areas chosen for audit. It is essential to develop a 'risk universe' consisting of the entire organisation's various risks—be they legal, compliance, regulatory, operational or IT—and to determine the correct priorities for audit based on the prevalent risk exposures.
- Auditors must have a defined/structured approach to handle all audits—from identification of areas to execution and reporting. The approach must be able to withstand any independent scrutiny. Undefined and informal approaches obviously invite unhappiness. It is better that they be based on industry standards or benchmarks.
- The methods used to conduct audits must be totally risk-based to avoid any potential bias. Adopting risk-based approaches will guarantee that each audit addresses all key and relevant risks. All the relevant risks must be identified. Once the relevant risks are identified, the corresponding controls to mitigate those risks must be listed. These lists of controls can be a desired list of controls, rather than a list to reflect the actual list of deployed controls. Once the desired list of controls is prepared, it must be compared with the actual controls on the field and any potential gaps identified. If material gaps exist, they should be reported. Unstructured methods will never be welcomed.
- At the same time, the controls must be tested for their effectiveness. Controls can be classified as preventive, detective or corrective. The controls should also be reasonable and commensurate to the risks that are to be mitigated. It is essential that the testing clearly identifies the efficiency and effectiveness of the controls in place. The audit must aim to identify clear gaps, if any, in the implementation of controls. If the auditor believes that better and alternate controls exist, the recommendations must clearly capture this need and outline the alternate requirements. However, the proposed changes must be articulated with facts and figures and without emotion.
- Auditors who produce reports—specifically, lengthy reports—that convey nothing will never be loved. Rather, reports must be produced in multiple formats to suit different audiences or they should encompass different sections, including a summary of issues, giving, in a nutshell, the essence of all the findings or observations.

- The auditor's observations must be factually accurate and must not be mere opinions. They must not lack objectivity, and they should not entertain anything subjective. Observations must be supported by adequate evidence gathered during the course of the audit. Observations should not be made if substantiation is not possible at a later date.
- Management of the areas audited must be given adequate opportunity to respond with their position on the audit report that goes out to leadership. They may differ with the observations made by the auditors; sometimes they may agree with the observations, but differ with the rating in terms of risk assigned to the findings. At times, they may agree with both, but may dispute the practicality or the pragmatic nature of the recommendations made by the auditors. Whatever the case may be, their point of view must be clearly recorded in the audit report, with no editing or alterations made to it by the auditors. Responses to such viewpoints must also be given equal prominence in the audit report. Any auditors who do not provide management an opportunity to respond and who fail to publish their responses are sure to be hated.
- Above all, it is essential to have auditors in place who do their job because they love to do it and are passionate about it. It should not be seen as a stop-gap arrangement in someone's career journey. Such agenda-centric auditors will clearly end up as targets for hate.
- To win better trust and confidence and to act as true business partners, it is essential that auditors follow up their audits with activities to make sure that the key issues get closed in an effective manner. Closure of critical issues must get validated.

Thus, there are a number of reasons why auditors can be hated. Sounds like a good subject for yet another book, right?

CPE Quiz

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

Quiz #132

Based on volume 3, 2010—Career Management in Turbulent Times

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

TRUE OR FALSE

SINGLETON ARTICLE

1. A key to IT audits of cloud computing and SaaS is to choose a framework for the components that assist an effective risk assessment of those technologies. Once a proper risk assessment is produced, the IT audit becomes a natural extension of auditing for the identified risks.

2. According to the Generally Accepted Accounting Principles (GAAP), if the infrastructure is outsourced, the expense associated with the IaaS infrastructure usually becomes a capital expense (CAPEX).

3. Security from unauthorized access by rogue employees of the IaaS provider is an increased risk to the user entity that needs to be addressed via adequate controls by the service entity.

4. In one sense, auditing cloud computing is like auditing any new IT—understand the IT, identify the risks, evaluate mitigating controls and audit the risky objects.

NEWMAN ARTICLE

5. During the evolution of the security function, security was a full-time role filled by IT practitioners who understood network technology.

6. A technology-oriented training approach is required to create in the next generation of security professionals the capability (with relevant skills and expertise) to respond quickly to guide the organization to a path that produces an acceptable level of risk.

7. Individuals often pursue certifications to enhance job prospects because many employers use them as benchmarks for hiring.

8. For every information security practitioner, risk analysis is a key requirement—not just an ability but a primary task, such as creating policies.

9. Security professionals must focus on negotiation and collaboration to work within the framework of the organization to ensure that risks are properly addressed.

10. An information security manager must make sure that the organization views security as a business function and the manager as a business partner.

BELL ARTICLE

11. Social psychology can assist an auditor's comprehension of how best to work with human predilections and predispositions to achieve the goal of improving security.

12. Understanding the social psychology of IT security auditing is equally as important as auditing processes and procedures.

13. An essential part of developing security awareness is to engage the auditee and allow the auditor to experience a paradigm shift—where auditors begin to comprehend the problems they intentionally create by their mere presence.

BROWN AND YARBERRY ARTICLE

14. Off-balance sheet exposure, collateralized debt obligations and many other factors are not included in comprehensive risk models.

15. An organization with low strategic agility risk may have siloed and disconnected applications, an excessive number of interorganizational links, and limited ability to change IT functionality within a reasonable time.

16. In today's environment in which disruption is nearly constant, only agile firms can shift products, offerings, services and suppliers fast enough to maintain or increase market share.

17. Agility is similar to factors such as morale, enthusiasm for one's work and job flexibility, which all strongly affect enterprise performance but are hard to measure. Although important, these are fuzzy. Hence, auditors cannot include agility in their assessment tool kit.

ISACA Journal

CPE Quiz

Based on volume 3, 2010—Career Management in Turbulent Times

Quiz #132 Answer Form

(Please print or type)

Name _____

_____

Address _____

_____

_____

CISA, CISM, CGEIT or CRISC # _____

Quiz #132

True or False

SINGLETON ARTICLE

1. _____
2. _____
3. _____
4. _____

NEWMAN ARTICLE

5. _____
6. _____
7. _____
8. _____
9. _____
10. _____

BELL ARTICLE

11. _____
12. _____
13. _____

BROWN AND YARBERRY ARTICLE

14. _____
15. _____
16. _____
17. _____

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

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

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

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

A passing score of 75 percent will earn one hour of CISA, CISM, CGEIT or CRISC CPE credit.

Answers—Crossword by Myles Mellor

See page 50 for the puzzle.

C	I	S	O	■	A	N	T	I	V	I	R	U	S	■
E	■	Y	■	A	■	I	■	■	I	■	■	R	O	I
R	I	S	K	M	A	N	A	G	E	R	■	L	O	T
T	■	T	■	B	■	E	■	R	■	A	■	■	N	■
■	M	E	R	I	T	■	■	C	U	T	U	P	■	T
C	■	M	■	T	A	B	■	■	N	E	■	E	A	R
H	U	S	H	■	■	I	N	S	I	D	E	R	■	O
A	■	■	■	I	S	O	■	■	T	■	■	Y	■	J
N	O	N	O	■	I	M	F	■	S	C	H	E	M	A
G	■	E	■	S	■	E	■	A	■	O	■	A	■	N
E	I	G	H	T	■	T	V	C	A	M	E	R	A	S
■	■	A	■	R	■	R	■	C	■	P	■	■	C	■
A	U	T	H	O	R	I	Z	E	D	U	S	E	R	S
D	■	E	■	N	■	C	■	S	I	T	■	R	E	P
D	E	S	I	G	N	S	■	S	P	E	A	R	■	Y

Standards Guidelines Tools and Techniques

ISACA MEMBER AND CERTIFICATION HOLDER COMPLIANCE

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

- **Standards** define mandatory requirements for IT audit and assurance.
  They inform:
  - IT audit and assurance professionals of the minimum level of acceptable performance required to meet the professional responsibilities set out in the ISACA Code of Professional Ethics
  - Management and other interested parties of the profession's expectations concerning the work of practitioners
  - Holders of the Certified Information Systems Auditor™ (CISA®) designation of requirements. Failure to comply with these standards may result in an investigation into the CISA holder's conduct by the ISACA Board of Directors or appropriate ISACA committee and, ultimately, in disciplinary action.
- **Guidelines** provide guidance in applying IT Audit and Assurance Standards. The IT audit and assurance professional should consider them in determining how to achieve implementation of the standards, use professional judgement in their application and be prepared to justify any departure. The objective of the IT Audit and Assurance Guidelines is to provide further information on how to comply with the IT Audit and Assurance Standards.
- **Tools and Techniques** provide examples of procedures an IT audit and assurance professional might follow in an audit engagement. The procedure documents provide information on how to meet the standards when performing IT auditing work, but do not set requirements. The objective of the IT Audit and Assurance Tools and Techniques is to provide further information on how to comply with the IT Audit and Assurance Standards.

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

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

The titles of issued standards documents are:

IT Audit and Assurance Standards
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

IT Audit and Assurance Guidelines
G1 Using the Work of Other Experts Effective 1 March 2008
G2 Audit Evidence Requirement Effective 1 May 2008
G3 Use of Computer-assisted Audit Techniques (CAATs) Effective 1 March 2008
G4 Outsourcing of IS Activities to Other Organisations Effective 1 May 2008
G5 Audit Charter Effective 1 February 2008
G6 Materiality Concepts for Auditing Information Systems Effective 1 May 2008
G7 Due Professional Care Effective 1 March 2008
G8 Audit Documentation Effective 1 March 2008
G9 Audit Considerations for Irregularities Effective 1 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 October 2008
G15 Audit Planning Revised Effective 1 Ma1 2010
G16 Effect of Third Parties on an Organisation's IT Controls Effective 1 March 2009
G17 Effect of Non-audit Role on the IS Auditor's Independence Effective 1 May 2010
G18 IT Governance Effective 1 May 2010
G19 Withdrawn 1 September 2008
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 October 2008
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 Re-engineering (BPR) Project Reviews Effective 1 July 2004
G27 Mobile Computing Effective 1 September 2004
G28 Computer Forensics Effective 1 September 2004
G29 Post-implementation Review Effective 1 January 2005
G30 Competence Effective 1 June 2005
G31 Privacy Effective 1 June 2005
G32 Business Continuity Plan (BCP) Review From IT Perspective Effective 1 September 2005
G33 General Considerations for the Use of the Internet Effective 1 March 2006
G34 Responsibility, Authority and Accountability Effective 1 March 2006
G35 Follow-up Activities Effective 1 March 2006
G36 Biometric Controls Effective 1 February 2007
G37 Configuration and Release Management Effective 1 November 2007
G38 Access Controls Effective 1 February 2008
G39 IT Organisation Effective 1 May 2008
G40 Review of Security Management Practices Effective 1 October 2008
G41 Return on Security Investment (ROSI) Effective 1 May 2010
G42 Continuous Assurance Effective 1 May 2010

IT Audit and Assurance Tools and Techniques
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 2005
P11 Electronic Funds Transfer (EFT) Effective 1 May 2007

Standards for Information System Control Professionals Effective 1 September 1999
510 Statement of Scope
.010 Responsibility, Authority and Accountability
520 Independence
.010 Professional Independence
.020 Organisational Relationship
530 Professional Ethics and Standards
.010 Code of Professional Ethics
.020 Due Professional Care
540 Competence
.010 Skills and Knowledge
.020 Continuing Professional Education
550 Planning
.010 Control Planning
560 Performance of Work
.010 Supervision
.020 Evidence
.030 Effectiveness
570 Reporting
.010 Periodic Reporting
580 Follow-up Activities
.010 Follow-up

Code of Professional Ethics Revised May 2003

Advertisers/Web Sites

Autonomy	*www.autonomy.com/compliance*	**3**
CCH Teammate	*www.CCHTeamMate.com*	**Inside Back Cover**
Citrix Online	*www.gotoassist.com/isaca*	**10**
ExamMatrix	*www.ExamMatrix.com/ISJ*	**5**
IAD Solutions	*www.AuditLeverage.com*	**19**
Modulo Risk Manager	*www.modulo.com*	**1**
University of Maryland University College	*www.umuc.edu/cyberedge*	**9**
Visual Click	*www.visualclick.com*	**6**

*** Position openings/recruitment listings**

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

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

ISSN 1944-1967

Leaders and Supporters

ISACA Bookstore

Resources for your Professional Development

Over 300 titles are available for sale through the ISACA® Bookstore. This insert highlights the new ISACA research and peer-reviewed books. See *www.isaca.org/bookstore* for the complete ISACA Bookstore listings.

2010 CISA® EXAM REFERENCE MATERIALS

See *www.isaca.org/cisabooks* to prepare for the December 2010 CISA exam.

CISA REVIEW MANUAL 2010

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

CISA REVIEW QUESTIONS, ANSWERS & EXPLANATIONS MANUAL 2010

QAE-10 English Edition (800 Questions)
QAE-10I Italian Edition (800 Questions)
QAE-10J Japanese Edition (800 Questions)
QAE-10S Spanish Edition (800 Questions)

CISA REVIEW QUESTIONS, ANSWERS & EXPLANATIONS MANUAL 2010 SUPPLEMENT

QAE-10ES English Edition (100 Questions)
QAE-10FS French Edition (100 Questions)
QAE-10IS Italian Edition (100 Questions)
QAE-10JS Japanese Edition (100 Questions)
QAE-10SS Spanish Edition (100 Questions)

CISA PRACTICE QUESTION DATABASE V10

(900 Questions)
CDB-10 CD-ROM—English Edition
CDB-10W Download—English Edition
(no shipping charges apply to download)
CDB-10S CD-ROM—Spanish Edition
CDB-10SW Download—Spanish Edition
(no shipping charges apply to download)

CANDIDATE'S GUIDE TO THE CISA EXAM AND CERTIFICATION

CAN
(No charge to paid CISA exam registrants)

2010 CISM® EXAM REFERENCE MATERIALS

See *www.isaca.org/cismbooks* to prepare for the December 2010 CISM exam.

CISM REVIEW MANUAL 2010

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

CISM REVIEW QUESTIONS, ANSWERS & EXPLANATIONS MANUAL 2010 SUPPLEMENT

(100 Questions)
CQA-10ES English (100 questions)
CQA-10JS Japanese Edition (100 questions)
CQA-10SS Spanish Edition (100 questions)

CISM REVIEW QUESTIONS, ANSWERS & EXPLANATIONS MANUAL 2009

CQA-9 English Edition (450 questions)
CQA-9J Japanese Edition (450 questions)
CQA-9S Spanish Edition (450 questions)

CISM REVIEW QUESTIONS, ANSWERS & EXPLANATIONS MANUAL 2009 SUPPLEMENT

CQA-9ES English Edition (100 questions)
CQA-9JS Japanese Edition (100 questions)
CQA-9SS Spanish Edition (100 questions)

CISM PRACTICE QUESTION DATABASE V10

(650 QUESTIONS)
MDB-10 CD-ROM—English Edition
MDB-10W Download—English Edition
(no shipping charges apply to download)

CANDIDATE'S GUIDE TO THE CISM EXAM AND CERTIFICATION

CGC
(No charge to paid CISM exam registrants)

2010 CGEIT EXAM REFERENCE MATERIAL

See *www.isaca.org/cgeitbooks* or *www.isaca.org/cgeitreferences* to prepare for the December 2010 CGEIT exam.

CGEIT REVIEW MANUAL 2010

CGM-10 English Edition

CANDIDATE'S GUIDE TO THE CGEIT EXAM AND CERTIFICATION

CACG
(No charge to paid CGEIT exam registrants)

COBIT®

See *www.isaca.org/cobitbooks* for complete descriptions and additional titles.

COBIT® 4.1

IT Governance Institute

COBIT is an IT governance framework and supporting tool set that allows managers to bridge the gap between control requirements, technical issues and business risks. COBIT enables clear policy development and good practice for IT control throughout organizations. COBIT was first published by ITGI in April 1996. ITGI's latest update—COBIT® 4.1—emphasizes regulatory compliance, helps organizations to increase the value attained from IT, highlights links between business and IT goals, and simplifies implementation of the COBIT framework. COBIT 4.1 is a fine-tuning of the COBIT framework and can be used to enhance work already done based upon earlier versions of COBIT. When major activities are planned for IT governance initiatives, or when an overhaul of the enterprise control framework is anticipated, it is recommended to start fresh with COBIT 4.1. COBIT 4.1 presents activities in a more streamlined and practical manner so continuous improvement in IT governance is easier than ever to achieve. 2007, 196 pages. **CB4.1**

COBIT AND APPLICATION CONTROLS: A MANAGEMENT GUIDE

ISACA

COBIT and Application Controls is structured based on the life cycle of application systems—from defining requirements through providing assurance on application controls. The concepts presented apply to new and existing legacy application systems. The book also offers guidance on:

- The definition and nature of application controls (addressing the six application controls discussed in COBIT)
- The design and operation of application controls
- Relationships and dependencies that application controls have with other controls, such as IT general controls
- The responsibilities of business and IT management

This guide helps business executives, business and IT managers, IT developers and implementers, and internal and external auditors implement, manage and provide assurance regarding application controls. 2009, 101 pages. **CAC**

COBIT SECURITY BASELINE, 2ND EDITION

IT Governance Institute

This publication focuses on IT security risk in a way that is simple to follow and implement for everyone, from the home user or small-to medium-sized enterprise to executives and board members of larger organizations. *COBIT® Security Baseline* provides an introduction to information security; an explanation of why security is important; the COBIT-based security baseline, mapped to ISO/IEC 27002; information security "survival kits" for varying audiences; and a summary of technical security risks. 2007, 48 pages. **CBSB2**

COBIT CONTROL PRACTICES: GUIDANCE TO ACHIEVE CONTROL OBJECTIVES FOR SUCCESSFUL IT GOVERNANCE, 2ND EDITION

IT Governance Institute

Control practices are derived from each control objective and help management, service providers, end users and control professionals to justify and design the specific controls needed to improve IT governance. The control practices provide the how, why and what to implement for each control objective, to improve IT performance and/or address IT solution and service delivery risks. By providing guidance on why controls are needed and what the best practices are for meeting specific control objectives, *COBIT® Control Practices* helps ensure that solutions put forward are likely to be more completely and successfully implemented. *COBIT® Control Practices* presents the key control mechanisms that support the achievement of control objectives. 2007, 174 pages. **CPS2**

COBIT QUICKSTART, 2nd EDITION

IT Governance Institute

COBIT® Quickstart is specifically designed to assist in rapid and easy adoption of the most essential elements of COBIT. *Quickstart* is a summarized version of the COBIT resources, focusing on the most crucial IT processes, control objectives and metrics, all presented in an easy-to-follow format to help users gain the benefits of COBIT quickly. *Quickstart* was designed as a baseline for many small to medium enterprises, but is also suitable for large organizations as a tool to accelerate adoption of IT governance best practices. *Quickstart* will help you to rapidly understand the important issues and management priorities. It can be followed by nontechnical people or managers who want principles, not detail, and is a useful springboard to the more comprehensive COBIT guidance. 2007, 58 pages. **CBQ2**

COBIT USER GUIDE FOR SERVICE MANAGERS

IT Governance Institute

This is the first of a planned series aimed at providing specific guidance on how to use COBIT when performing a particular role. The first publication is focused on the service manager, as it is known that this is a significant role where there is a high demand for guidance. Each guide will highlight a specific group of COBIT users and describe how to use COBIT to support their activities, how to focus on the parts of COBIT that are most relevant to them, and how COBIT relates to the best practices and standards that they would typically use in their job. This guide contains an introduction to the business and governance challenges facing service managers and describes how COBIT can help, an explanation of the service manager role and why it is important for effective IT governance, the key governance tasks for the role aligned with the ITIL V3 processes and COBIT 4.1 control objectives, case examples, a high level maturity model for the role area, and links to other references. 2009, 54 pages. **CUG**

IMPLEMENTING AND CONTINUALLY IMPROVING IT GOVERNANCE

ISACA

Replacing the popular *IT Governance Implementation Guide*, this publication assists enterprises in establishing and sustaining an effective approach to governing IT.

New features include Risk IT-related content as well as typical pain points that new or improved IT governance practices can help solve, including outsourcing service delivery problems and business frustration with failed initiatives.

Implementing and Continually Improving IT Governance is based on a life cycle of continuous improvement. In addition to describing the steps that need to be considered and undertaken to progress an IT governance initiative, this guide identifies trigger events that indicate the need for better governance, as well as implementation challenges enterprises might face. It also describes how to use COBIT, Val IT and Risk IT components for critical support. 2009, 78 pages. **ITG9**

IT ASSURANCE GUIDE: USING COBIT

IT Governance Institute

Management needs assurance that the desired IT goals and objectives are being met and that key controls are in place and effective. The *IT Assurance Guide* introduces the various types of IT assurance activities that exist and describes how COBIT can be used to support such activities. It provides invaluable guidance for assurance professionals and a structured assurance approach linked to the COBIT framework that provides a common language and criteria for business and IT people. This approach facilitates a shared identification of control priorities and improvements.
2007, 269 pages. **CB4A**

SHAREPOINT DEPLOYMENT AND GOVERNANCE USING COBIT 4.1: A PRACTICAL APPROACH

NEW

Dave Chennault and Chuck Strain

SharePoint has quickly become one of Microsoft's most successful products and the *de facto* collaboration standard. But deployment is often accompanied by chaos and a wave of frustration called "the SharePoint Effect" as organizations become overwhelmed by their own success, a lack of planning or insufficient governance. While many bloggers and self-appointed experts have offered "best practice" guidelines, *SharePoint Deployment and Governance Using COBIT 4.1* contains a comprehensive, step-by-step guide on how to practically deploy and govern SharePoint 2007 and 2010 using COBIT 4.1, the leading internationally accepted governance framework.

(cont. p.S-2)

This practical guide blends the needs of the deployment staff and audit teams with a comprehensive blueprint that puts business in charge. The book is filled with authoritative tips, techniques and advice on:
- How to use COBIT 4.1 for SharePoint deployment and governance—on premises or in the cloud
- Specific considerations when using SharePoint 2007 or SharePoint 2010
- Which third-party tools to consider to govern your SharePoint farm
- How to apply appropriate COBIT processes at each stage of the SharePoint deployment

2010, 176 pages. **SDG**

RISK IT AND RISK RELATED TOPICS

See *www.isaca.org/riskitbooks* for additional information.

INFORMATION TECHNOLOGY RISK MANAGEMENT IN ENTERPRISE ENVIRONMENTS

NEW

Jake Kouns and Daniel Minoli

This book provides a comprehensive review of industry approaches, practices and standards on how to handle the ever-increasing risks to organizations' business-critical assets. Through a practical approach, this book explores key topics that enable readers to uncover and remediate potential infractions. The authors present an effective risk management program by providing:
- An overview of risk assessment, mitigation and management approaches and methodologies
- Processes for developing a repeatable program for technological issues and human resources
- Definitions of key concepts and security standards in the area of risk management
- Analytical techniques for assessing the amount of risk and the benefit of risk remediation
- Information on the development and implementation of a risk management team

The book details fundamental corporate risks and outlines how they can be avoided. It is an essential resource for information security managers and analysts, system developers, auditors, consultants, and students in understanding the IT resources, procedures and tools to identify and handle technology and security risks.
2010, 421 pages. **84-WRM**

THE RISK IT FRAMEWORK

ISACA

The Risk IT Framework provides a set of guiding principles and supporting practices for enterprise management, combined to deliver a comprehensive process model for governing and managing IT risk. For users of COBIT and Val IT, this process model will look familiar. Guidance is provided on the key activities within each process, responsibilities for the process, information flows between processes and performance management of each process. The model is divided into three domains—Risk Governance, Risk Evaluation, Risk Response—each containing three processes:
- Risk Governance
- Risk Evaluation
- Risk Response

2009, 104 pages. **RITF**

THE RISK IT PRACTITIONER GUIDE

ISACA

The Risk IT Practitioner Guide, a support document for the Risk IT framework, provides examples of possible techniques to address IT-related risk issues, and more detailed guidance on how to approach the concepts covered in the process model.

Concepts and techniques explored in more detail include:
- Building enterprise-specific scenarios, based on a set of generic IT risk scenarios
- Building a risk map, using techniques to describe the impact and frequency of scenarios
- Building impact criteria with business relevance
- Defining key risk indicators (KRIs)
- Using COBIT and Val IT to mitigate risk; the link between risk and COBIT control objectives and Val IT key management practices

2009, 134 pages. **RITPG**

Val IT™

See *www.isaca.org/valitbooks* for complete descriptions.

Val IT is the most complete collection of proven management practices and techniques for investment in IT-enabled business change and innovation. IT allows enterprises to increase return on their investments and generate business value. IT helps enterprises to make better decisions on where to invest in business change—ensuring they are doing the right things the right way, doing them well and getting benefits from them. Val IT fosters the partnership between IT and the rest of business.

THE VAL IT FRAMEWORK 2.0

ISACA

This publication is the foundation document in the Val IT series. It presents practices for three domains:
- Value Governance
- Portfolio Management
- Investment Management

Each of these domains is broken down into key management processes and a number of key management practices.

This edition simplifies the management processes and practices, and extends the Val IT Framework beyond new investments to include IT services, assets and other resources. It also aligns terminology with COBIT, and adds a management guidelines section, similar to COBIT, which provides a greater level of detail on the Val IT processes, key management practices and maturity models for each Val IT domain.
2008, 146 pages. **VITF2**

GETTING STARTED WITH VALUE MANAGEMENT

ISACA

This is a guide that outlines "how to implement" Val IT and compliments the *The Val IT Framework,* which describes "what you do." *Getting Started With Value Management* is made up of six chapters that flow in a logical sequence moving from typical starting points, pain points or "trigger points" to specific approaches to address these points.

It offers assessment templates and practical guidance on how to use the new framework, along with recommended approaches to addressing investment issues in organizations. It contains suggested maturity models and approaches to maintaining and sustaining change.
2008, 44 pages. **VITM**

VALUE MANAGEMENT GUIDANCE FOR ASSURANCE PROFESSIONALS—USING VAL IT 2.0

NEW

ISACA

The objective of the newest publication to the Val IT family *Value Management Guidance for Assurance Professionals—Using Val IT 2.0* is to provide guidance on how to use Val IT to support an assurance review focused on the governance of IT-enabled business investments for each of the three Val IT domains—Value Governance, Portfolio Management and Investment Management. This guide is based on the *IT Assurance Guide Using COBIT* which provides comprehensive guidance on planning and performing a wide range of IT related assurance activities. This guide is focused on an assurance review of IT value management based on and aligned with the *Val IT 2.0 Framework*—the governance of IT related business investments. Readers should be familiar with Val IT 2.0. Readers wishing to obtain a fuller description and understanding of IT assurance principles and context should refer to the *IT Assurance Guide: Using COBIT.*
2010, 48 pages. **VITAG**

THE BUSINESS CASE GUIDE—USING VAL IT 2.0

NEW

ISACA

The intention of this publication is to position the business case as a valuable management tool—an operational tool—and to provide an easy-to-follow guide, based on Val IT 2.0, to creating, maintaining and using the business case. As such, this publication builds on and enhances the earlier version of this guide, *Enterprise Value: Governance of IT Investments, The Business Case* (2006). This new publication is now fully aligned with Val IT 2.0, provides "how to do it" tips, maturity models, examples and references to other materials for using and implementing the business case processes as the powerful operational tools they have the potential to be.
2010, 49 pages. **VITB2**

AUDIT, CONTROL AND SECURITY—ESSENTIALS

See *www.isaca.org/essentialsbooks* for complete descriptions and additional essential titles.

ACCOUNTING INFORMATION SYSTEMS, 8TH EDITION

NEW

Ulric J. Gelinas, Richard B. Dull

Today's accounting professionals must help organizations identify enterprise risks and provide assurance for information systems. *Accounting Information Systems, 8th Edition*, helps develop a solid foundation in enterprise risk management as it relates to business processes and information systems. The book's proven coverage centers around three of the areas most critical in accounting information systems today: enterprise systems, e-business systems and controls for maintaining those systems. The book is written clearly to help readers easily grasp even the most challenging topics. It explores today's most intriguing AIS topics to see how they relate to business processes, information technology, strategic management, security and internal controls.

ISACA member complimentary PDF *www.isaca.org/downloads*

The eighth edition provides the tools and processes for organizing and managing information. Whether desiring an emphasis on enterprise risk management, a solid understanding of databases and REA, or a background in systems development, this book offers a solid foundation. 2010, 696 pages **1-IT8**

COMPUTER SECURITY, PRIVACY AND POLITICS: CURRENT ISSUES, CHALLENGES AND SOLUTIONS

NEW

Ramesh Subramanian

The intersection of politics, law, privacy and security in the context of computer technology is both sensitive and complex. Computer viruses, worms, Trojan horses, spyware, computer exploits, poorly designed software, inadequate technology laws, politics and terrorism—all of these have a profound effect on our daily computing operations and habits, with major political and social implications.

Computer Security, Privacy and Politics: Current Issues, Challenges and Solutions connects privacy and politics, offering a point-in-time review of recent developments in computer security. This reference source compiles content on such topics as reverse engineering of software, understanding emerging computer exploits, emerging lawsuits and cases, global and societal implications, and protection from attacks on privacy. 2008, 356 pages. **4-IGI**

EFFECTIVE PROJECT MANAGEMENT: TRADITIONAL, AGILE, EXTREME, 5TH EDITION

NEW

Robert K. Wysocki

The fifth edition of this popular guide gives new or veteran project managers a comprehensive overview of all of the best-of-breed project management approaches and tools today, including traditional (linear and incremental), agile (iterative and adaptive) and extreme. Step-by-step instruction and practical case studies show you how to use these tools effectively to achieve better outcomes. Plus, the book provides full coverage on managing continuous process improvement, procurement, distressed projects and multiple team projects.
2009, 792 pages. **50-WPM5**

FRAUD ANALYSIS TECHNIQUES USING ACL

David Coderre

Fraud Analysis Techniques Using ACL offers auditors and investigators:
- Authoritative guidance on the use of computer-assisted audit tools and techniques in fraud detection
- A CD-ROM containing an educational version of ACL
- An accompanying CD-ROM containing a thorough fraud tool kit with two sets of customizable scripts to serve your specific audit needs
- Case studies and sample data files that you can use to try out the tests
- Step-by-step instructions on how to run the tests
- A self-study course on ACL script development with exercises, data files and suggested answers

The tool kit also contains 12 utility scripts and a self-study course on ACL scripting, which includes exercises, data files and proposed answers. Filled with screen shots, flow charts, example data files, descriptive commentary highlighting and explaining each step, and case studies offering real-world examples of how the scripts can be used to search for fraud, it is the only tool kit you will need to harness the power of ACL to spot fraud. 2009, 176 pages, CD-ROM included. **82-WACL**

GFI NETWORK SECURITY AND PCI COMPLIANCE POWER TOOLS

NEW

Brien Posey

Today all companies, US federal agencies and nonprofit organizations have valuable data on their servers that need to be secured. One of the challenges for IT experts is learning how to use new products in a time-efficient manner, so that new implementations can go quickly and smoothly. Learning how to set up sophisticated products is time-consuming and can be confusing. GFI's LANguard Network Security Scanner reports vulnerabilities so that they can be mitigated before unauthorized intruders can wreak havoc on the network. To take advantage of the best things that GFI's LANguard Network Security Scanner has to offer, it should be configured on the network so that it captures key events and sends alerts regarding potential vulnerabilities before they are exploited. This book pinpoints the most important concepts with examples and screenshots so that systems administrators and security engineers can understand how to get the GFI security tools working quickly and effectively.
2009, 488 pages. **10-EL**

INFORMATION STORAGE AND MANAGEMENT: STORING, MANAGING, AND PROTECTING DIGITAL INFORMATION

NEW

EMC

Managing and securing information is critical to business success. While information storage and management used to be a relatively straightforward and routine operation, it has developed into a highly mature and sophisticated pillar of information technology. Information storage and management technologies provide a variety of solutions

for storing, managing, connecting, protecting, securing, sharing and optimizing information.

To keep pace with the exponential growth of information and the associated increase in sophistication and complexity of information management technology, there is a growing need for skilled information management professionals. More than ever, IT managers are challenged with employing and developing highly skilled information storage professionals. 2009, 480 pages. **83-WIS**

ITAF: A PROFESSIONAL PRACTICES FRAMEWORK FOR IT ASSURANCE
ISACA

ITAF: A Professional Practices Framework for IT Assurance consists of compliance and good practice setting guidance. The IT Assurance Framework™ (ITAF™):
- Provides direction on the design, conduct and reporting of IT audit and assurance assignments
- Defines terms and concepts specific to IT assurance
- Establishes standards that address IT audit and assurance professional roles and responsibilities, knowledge, skills and diligence, conduct, and reporting requirements

ITAF provides a single source through which IT audit and assurance professionals can seek guidance, research policies and procedures, obtain audit and assurance programs, and develop effective reports. 2008, 71 pages. **WITAF**

PCI COMPLIANCE, SECOND EDITION
Anton Chuvakin and Branden R. Williams

Identity theft and other confidential information theft has now topped the charts as the number one cybercrime. In particular, credit card data are preferred by cybercriminals. Is your payment processing secure and compliant? This book is packed with help to develop and implement an effective security strategy to keep infrastructure compliant and secure. Now in its second edition, *PCI Compliance* is revised to follow the new Payment Card Industry Data Security Standard (PCI DSS) 1.2.1. Also new in this edition, each chapter has how-to guidance to walk you through implementing concepts and real-world scenarios to help you relate to the information better and grasp how it impacts your data. This book will provide the information needed to understand the current PCI DSS standards and how to effectively implement security on the network infrastructure in order to be compliant with the credit card industry guidelines and protect sensitive and personally identifiable information. 2009, 368 pages. **7-SYN9**

AUDIT, CONTROL AND SECURITY—SPECIFIC ENVIRONMENTS

See *www.isaca.org/specificbooks* for complete descriptions and additional specific environment titles.

APPLIED ORACLE SECURITY: DEVELOPING SECURE DATABASE AND MIDDLEWARE ENVIRONMENTS
NEW
David Knox, Scott Gaetjen, Hamza Jahangir, Tyler Muth, Patrick Sack, Richard Wark and Bryan Wise

This Oracle Press guide demonstrates practical applications of the most compelling methods for developing secure Oracle Database and Oracle Middleware environments. You will find full coverage of the latest and most popular Oracle products, including Oracle Database and Audit Vaults, Oracle Application Express, and secure Business Intelligence applications.

Applied Oracle Security demonstrates how to build and assemble the various Oracle technologies required to create the sophisticated applications demanded in today's IT world. Most technical references only discuss a single product or product suite. As such, there is no road map to explain how to get one product, product family or suite to work with another. This book fills that void with respect to Oracle Middleware and Oracle Database products and the area of security. 2009, 640 pages **18-MAO**

SECURITY, AUDIT AND CONTROL FEATURES ORACLE® E-BUSINESS SUITE, 3RD EDITION
NEW
ISACA

This updated edition of one of ISACA's most popular guides reflects the many changes that the business environment and Oracle ERP application have undergone since the second edition was published. In response to customer needs and an increased market awareness of governance, risk and compliance (GRC), Oracle Corporation has continued to boost its GRC offerings and released the updated and improved Oracle E-Business Suite R12.1 (EBS) in 2009. *Security, Audit and Control Features Oracle® E-Business Suite, 3rd Edition* reflects these new developments to provide a current view regarding:
- How business processes impact ERP implementation and operation
- Application functionality
- Strategic business risk
- Technical system architecture
- Security and control criteria/drivers for key functional areas, including:
  - Financial accounting
  - Expenditures
  - Web-enabled security
- IT resource requirements
- IT management requirements
- Professional services and support
- IT integration with other enterprise systems
- Organizational and audit department challenges with Oracle E-Business Suite
- Oracle E-Business audit programs
- Using Oracle to assist with the regulatory requirements of financial reporting and other compliance issues
- How Oracle's GRC offering integrates with Oracle E-Business Suite

This in-demand guide also provides an update on current industry standards and identifies future trends in Oracle EBS risk and control. It enables audit, assurance, risk and security professionals (IT and non-IT) to evaluate risks and controls in existing ERP implementations, and facilitate the design and implementation of better practice controls into system upgrades and enhancements. This book also aims to assist system architects, business analysts and business process owners who are implementing Oracle EBS, as well as people responsible for managing it in live production to maintain the appropriate level of control and security according to business needs and industry standards. 2010, 407 pages. **ISOA3**

SECURITY, AUDIT AND CONTROL FEATURES ORACLE® DATABASE, 3RD EDITION
ISACA

Security, Audit and Control Features Oracle Database, 3rd Edition, provides a new perspective of security and controls over Oracle. This updated edition includes a background and review of security controls and addresses the risks associated with protecting information in a distributed computing environment of various platforms, versions, interfaces and tools.

The goal of this popular book is to guide the assessor through a comprehensive evaluation of security for an Oracle database based on business objectives and risks. It examines several different frameworks that can be used to assess security risks and covers technical topics, including an overview of Oracle Database's architecture, operating system controls, auditing and logging, network security, and new features in Oracle 11*g* (differences from previous versions of Oracle Database are noted, as well as differences that may exist based on the host operating system of the database).

Security, Audit and Control Features Oracle® Database helps simplify a daunting task, giving readers the approach, knowledge and tools to effectively plan and execute an Oracle Database security assessment. 2009, 219 pages. **ODB9**

SECURITY, AUDIT AND CONTROL FEATURES SAP® ERP: TECHNICAL AND RISK MANAGEMENT REFERENCE SERIES, 3RD EDITION
Deloitte Touche Tohmatsu Research Team and ISACA

Security, Audit and Control Features SAP® ERP, 3rd Edition, part of the Technical and Risk Management Reference Series, enables assurance, security and risk professionals to evaluate risks and controls in existing ERP implementations and facilitates the design and building of controls into system upgrades and enhancements.

The publication is based on SAP ERP (also known as SAP ERP Central Component [ECC]), the latest version of which is SAP ECC 6.0.

This in-demand new edition has been updated to reflect:
- New/modified SAP transaction codes and reports
- SAP ERP based on a service-oriented architecture (SOA). SOA combines SAP ERP with an open technology platform that can integrate SAP and non-SAP systems using the SAP Netweaver platform.
- SAP GRC suite of tools, including Access Control and Process Control, which offers corporate governance and risk management solutions

2009, 470 pages. **ISAP3**

NON-ENGLISH RESOURCES

See *www.isaca.org/nonenglishbooks* for complete descriptions and additional non-English titles.

AUDITORÍA DE TECNOLOGÍAS Y SISTEMAS DE INFORMACIÓN.
Piattini, M. y otros

2008, 732 Págs. **3-RAMA**

CISA EXAMINATION REFERENCE MATERIAL
Study aids available in French, Italian, Japanese and Spanish for the December 2010 CISA exam—see page S5

CISM EXAMINATION REFERENCE MATERIAL
Study aids available in Japanese and Spanish for the December 2010 CISM exam—see page S5

COMPUTACIÓN FORENSE: DESCUBRIENDO LOS RASTROS INFORMÁTICOS
Jeimy Cano

2009, 340 pages. **1-AOCF**

GOBIERNO DE LAS TECNOLOGÍAS Y LOS SISTEMAS DE INFORMACIÓN
M. Piattini y F. Hervada

2007, 489 Págs. **2-RAMA**

SECURITY, AUDIT AND CONTROL FEATURES ORACLE E-BUSINESS SUITE: A TECHNICAL AND RISK MANAGEMENT REFERENCE GUIDE
Japanese Edition. 2006, 368 pages. **ISOAJ**

SECURITY, AUDIT AND CONTROL FEATURES SAP R/3: A TECHNICAL AND RISK MANAGEMENT REFERENCE GUIDE
Japanese Edition. 2006, 255 pages. **ISAPJ**

INTERNET AND RELATED SECURITY TOPICS

See *www.isaca.org/internetbooks* for complete descriptions and additional Internet and related security titles.

24 DEADLY SINS OF SOFTWARE SECURITY: PROGRAMMING FLAWS AND HOW TO FIX THEM
NEW
Michael Howard, David LeBlanc and John Viega

Fully updated to cover the latest security issues, *24 Deadly Sins of Software Security* reveals the most common design and coding errors and explains how to fix each one—or better yet, avoid them from the start. This book has been completely revised to address the most recent vulnerabilities and has added five brand-new sins. This practical guide covers all platforms, languages and types of applications. Eliminate these security flaws from your code:
- SQL injection
- Use of magic URLs, predictable cookies and hidden form fields
- Format string problems
- C++ catastrophes
- Command injection
- Information leakage
- Poor usability
- Executing code with too much privilege
- Insecure mobile code
- Weak random numbers
- Failing to protect network traffic
- Trusting network name resolution

2009, 432 pages **19-M24**

CLOUD COMPUTING: IMPLEMENTATION, MANAGEMENT, AND SECURITY
John W. Rittinghouse and James F. Ransome

This guide provides an understanding of what cloud computing really means, explores how disruptive it may become in the future, and examines its advantages and disadvantages. It gives business executives the knowledge necessary to make informed, educated decisions regarding cloud initiatives. The authors first discuss the evolution of computing from a historical perspective, focusing primarily on advances that led to the development of cloud computing. They then survey some of the critical components that are necessary to make the cloud computing paradigm feasible. They also present various standards based on the use and implementation issues surrounding cloud computing and describe the infrastructure management that is maintained by cloud computing service providers. After addressing significant legal and philosophical issues, the book concludes with a hard look at successful cloud computing vendors.

Helping to overcome the lack of understanding currently preventing even faster adoption of cloud computing, this book arms readers with guidance essential to make smart, strategic decisions on cloud initiatives. 2009, 340 pages. **45-CRC**

COMPUTER AND INFORMATION SECURITY HANDBOOK
John Vacca

This book presents information on how to analyze risks to your networks and the steps needed to select and deploy the appropriate countermeasures to reduce your exposure to physical and network threats. It also imparts the skills and knowledge needed to identify and counter some fundamental security risks and requirements, including Internet security threats and measures (audit trails, IP sniffing/spoofing, etc.), and how to implement security policies and procedures.
In addition, this book also covers security and network design with respect to particular vulnerabilities and threats, risk assessment and mitigation, and auditing and testing of security systems. Coverage includes identifying vulnerabilities and implementing appropriate countermeasures to prevent and mitigate threats to mission-critical

processes. Techniques are explored for creating a business continuity plan (BCP) and the methodology for building an infrastructure that supports its effective implementation. The book provides essential knowledge and skills needed to select, design and deploy a public key infrastructure to secure existing and future applications and includes a discussion of vulnerability scanners to detect security weaknesses and prevention techniques, as well as allowing access to key services while maintaining systems security. 2009, 928 pages. **9-EL**

HACKING EXPOSED COMPUTER FORENSICS SECRETS AND SOLUTIONS, 2ND EDITION NEW

Aaron Philipp, David Cowen and Chris Davis

Identify and investigate computer criminals of all stripes with help from this fully updated, real-world resource. This edition explains how to construct a high-tech forensic lab, collect prosecutable evidence, discover e-mail and system file clues, track wireless activity, and recover obscured documents. Learn how to re-create an attacker's footsteps, communicate with council, prepare court-ready reports, and work through legal and organizational challenges. Case studies straight from recent headlines cover IP theft, mortgage fraud, employee misconduct, securities fraud, embezzlement, organized crime and consumer fraud cases. 2009, 544 pages. **1-MHF**

NETWORK SECURITY BIBLE, 2ND EDITION NEW

Eric Cole

Network security is constantly evolving, and this comprehensive guide has been thoroughly updated to cover the newest developments. Those responsible for network security will find value in this is reference. Covering new techniques, technology and methods for approaching security, it also examines new trends and best practices being used by many organizations. It is fully revised to address new techniques, technology and methods for securing an enterprise worldwide and features additional chapters on areas related to data protection/ correlation and forensics. 2009, 936 pages. **86-WNS**

SCRAPPY INFORMATION SECURITY: THE EASY WAY TO KEEP THE CYBER WOLVES AT BAY NEW

Michael Seese

This book is written for those who care about the security and privacy of their online information, and want to know how to take steps to protect it. It will help readers to ensure that they do not inadvertently compromise their employer's, or their own, sensitive information. This book provides concrete steps to take to reduce cybercrime and minimize its impacts. 2009, 212 pages. **1-HA**

IT GOVERNANCE AND BUSINESS MANAGEMENT

See *www.isaca.org/managementbooks* for complete descriptions and additional IT governance and management titles.

ENTERPRISE INFORMATION SECURITY AND PRIVACY

C. Warren Axelrod, Jennifer Bayuk and Daniel Schutzer

This is a unique and practical book that addresses the rapidly growing problem of information security, privacy and secrecy threats and vulnerabilities. This authoritative resource helps the reader understand what really needs to be done to protect sensitive data and systems and how to comply with the burgeoning roster of data protection laws and regulations. The book examines the effectiveness and weaknesses of current approaches and guides the reader toward practical methods and doable processes that can bring about real improvement in the overall security environment. The reader will gain insight into the latest security and privacy trends, learn how to determine and mitigate risks, and discover the specific dangers and responses regarding the most critical sectors of a modern economy. 2009, 260 pages. **9-ART**

FRAUD 101: TECHNIQUES AND STRATEGIES FOR UNDERSTANDING FRAUD, 3RD EDITION NEW

Stephen Pedneault

Fraud continues to be one of the fastest growing and most costly crimes around the world. The more an organization can learn about fraud and the potential fraud risks that threaten the financial stability of the organization's cash flow, the better that organization will be equipped to design and implement measures to prevent schemes from occurring in the first place. This third edition offers guidance, understanding, and new, real-world case studies on the major types of fraud. 2009, 234 pages, **85-WF101**

Learn more about COBIT visit:

COBIT Home Page *www.isaca.org/cobit*

COBIT Online *www.isaca.org/cobitonline*

HACKING EXPOSED MALWARE AND ROOTKITS: MALWARE & ROOTKITS SECRETS & SOLUTIONS NEW

Michael A. Davis, Sean Bodmer, Aaron LeMasters

Defend against the ongoing wave of malware and rootkit assaults the "Hacking Exposed" way. Real-world case studies and examples reveal how today's hackers use readily available tools to infiltrate and hijack systems. Step-by-step countermeasures provide proven prevention techniques. Readers will find out how to detect and eliminate malicious embedded code, block pop-ups and web sites, prevent keylogging, and terminate rootkits. The latest intrusion detection, firewall, honeynet, antivirus, antirootkit and antispyware technologies are covered in detail. 2009, 400 pages **20-MHE**

INFORMATION SECURITY GOVERNANCE: GUIDANCE FOR INFORMATION SECURITY MANAGERS

W. Krag Brotby and IT Governance Institute

This book discusses how to develop an information security strategy within an organization's governance framework and how to drive that strategy through an information security program. It provides guidance on determining information security objectives and how to measure progress toward achieving them. It is an exposition on the rationale and necessity for senior management to integrate information security into overall organizational governance at the highest levels. It provides information, developed in recent years, that mandates a business case for information security governance. 2008, 78 pages. **3-ITG**

INFORMATION TECHNOLOGY GOVERNANCE AND SERVICE MANAGEMENT: FRAMEWORKS AND ADAPTATIONS NEW

Aileen Cater-Steel

Increasingly, IT governance is being considered an integral part of corporate governance. There has been a rapid increase in awareness and adoption of IT governance as well as a desire to conform to national governance requirements to ensure that IT is aligned with the objectives of the organization.

This book provides an in-depth view into the critical contribution of IT service management to IT governance, and the strategic and tactical value provided by effective service management. A must-have resource for practitioners in fields affected by IT in organizations, this work gathers authoritative perspectives on the state of research on organizational challenges and benefits in current IT governance frameworks, adoption and incorporation. Section 1 provides literature reviews of previous research on IT governance, and section 2 contains six case studies of IT governance. Section 3 provides perspectives on the relationship of IT governance to business, corporate governance and IT security. It also considers governance as it relates to IT portfolio management, outsourcing and software development. Section 4 describes models of IT service management such as ITIL and ISO/ IEC 2000. 2009, 519 pages. **3-IGI**

INTERNAL CONTROLS POLICIES AND PROCEDURES

Rose Hightower

Your company can use this how-to manual to quickly and effectively put a successful program of internal controls in place. Complete with flowcharts and checklists, this essential desktop reference is a best practices model for establishing and enhancing your organization's control framework.

Internal Controls Policies and Procedures is a collection of documents that summarize the regulations and rules which are part of corporate governance. It includes various definitions within the US Securities and Exchange Commission regulations, and the Sarbanes-Oxley Act and Public Company Accounting Oversight Board (PCAOB) and the American Institute of Certified Public Accountants (AICPA) standards, and an overview of the COSO framework.

The how-to reference shows how to establish or enhance an internal control program. This manual includes an integrated internal control program and series of assessment checklists. 2008, 272 pages. **81-WIC**

IT FINANCIAL MANAGEMENT

Maxime Sottini

It is now accepted that IT functions are a fundamental part of the competitive business model. Instead of simply offering services IT must create value for the business.
This practical publication describes the strong financial skills that IT managers must have in order to support:
- Operations
- Budgeting
- Project delivery
- Business modeling
- Investment and business cases

This book covers the main financial concepts that managers need to be familiar with in order for IT to take its proper place as a contributor to the business. It assumes a basic level of financial understanding and builds on the techniques required almost daily; therefore, it is overwhelmingly practical and based on real-world scenarios. The techniques are fully described, and issues such as roles, implementation, daily management and even tooling are detailed.
2009, 230 pages. **12-VH**

OUTSOURCING IT: A GOVERNANCE GUIDE NEW

Rupert Kendrick

Businesses are increasingly choosing to outsource their IT function. The attraction of outsourcing IT is that it enables a company to obtain an efficient and responsive IT system, while at the same time allowing the company to focus on its core strengths. The current economic climate is also putting companies under increasing pressure to find new ways of cutting costs. However, all too often IT outsourcing projects fail because companies have not applied appropriate governance processes to the project.

The IT function is nearly always a business-critical operation. This means that outsourcing IT will give a supplier control over a function that is vital to the organization's survival and success.

This book offers a guide to the many pitfalls of IT outsourcing. It will provide readers with clear criteria for the application of governance principles to the outsourcing process and, thereby, enable them to implement IT outsourcing so that it supports the overall business goals. 2009, 336 pages **2-ITO**

TECHNOLOGY SCORECARDS: ALIGNING IT INVESTMENTS WITH BUSINESS PERFORMANCE

Sam Bansal

Readers can learn how to establish key performance indicators and value scorecards for IT to ensure maximum value in their corporation with the step-by-step approach in *Technology Scorecards*. This book will show the reader how to:
- Create scorecards geared toward the enterprise's business goals
- Make quantum improvements in cost, value and productivity using key performance indicators and scorecards
- Increase a company's net by as much as 100 percent just by improving its supply chain management by 50 percent
- Impact the enterprise's top line the most through product life cycle management
- Develop a realistic strategy through scorecards, which can then be used to drive IT investments that maximize business performance

Readers can learn how to align their IT plans with business objectives and optimize the enterprise's overall performance with the perfect scorecard approach found in *Technology Scorecards*.
2009, 336 pages. **77-WTS**

UNLOCKING VALUE: AN EXECUTIVE PRIMER ON THE CRITICAL ROLE OF IT GOVERNANCE

IT Governance Institute

The goals of this publication are to:
- Increase awareness, understanding and adoption of IT governance by enabling chief information officers (CIOs) and other executives to better understand the why, what and how of IT governance
- Create a call to enterprises for the need to adopt the concepts of IT governance
- Assist CIOs in their effort to increase their enterprise's leadership awareness of the need to adopt the concepts of IT governance and obtain their support
- Assist CIOs in their effort to facilitate an understanding of the topic and obtain their buy-in and commitment
- Assist CIOs in their effort to provide leadership for successful implementation, adoption and execution of IT governance

2008, 28 pages. **4-ITG**

VULNERABILITY MANAGEMENT

Park Foreman

Vulnerability Management proactively shows how to prevent the exploitation of IT security and weaknesses that exist particularly with a large organization. Illustrated with examples drawn from more than two decades of multinational experience, the author demonstrates how much easier it is to manage potential weaknesses, than to clean up after a violation. Covering the diverse realms that chief officers need to know and the specifics applicable to singular areas of departmental responsibility, he provides both the strategic vision and action steps needed to prevent the exploitation of IT security gaps, especially those that are inherent in a larger organization. 2009, 347 pages. **44-CRC**

ISACA member complimentary PDF *www.isaca.org/downloads*

ISACA Bookstore Price List

Code	Title	Nonmember	Member

2010 CISA® EXAM REFERENCE MATERIALS

◆ *To prepare for the **December 2010** CISA exam, order* ◆

CISA Review Manual 2010*			
CRM-10	English Edition	$135.00	$105.00
CRM-10F	French Edition	135.00	105.00
CRM-10I	Italian Edition	135.00	105.00
CRM-10J	Japanese Edition	135.00	105.00
CRM-10S	Spanish Edition	135.00	105.00
CISA Review Questions, Answers & Explanations Manual 2010*			
QAE-10	English Edition (800 questions)	130.00	100.00
QAE-10I	Italian Edition (800 questions)	130.00	100.00
QAE-10J	Japanese Edition (800 questions)	130.00	100.00
QAE-10S	Spanish Edition (800 questions)	130.00	100.00
CISA Review Questions, Answers & Explanations Manual 2010 Supplement*			
QAE-10ES	English Edition (100 questions)	60.00	40.00
QAE-10FS	French Edition (100 questions)	60.00	40.00
QAE-10IS	Italian Edition (100 questions)	60.00	40.00
QAE-10JS	Japanese Edition (100 questions)	60.00	40.00
QAE-10SS	Spanish Edition (100 questions)	60.00	40.00
CISA Practice Question Database v10 (900 questions)*			
CDB-10	CD-ROM—English Edition	225.00	185.00
CDB-10W	Download—English Edition (No shipping charges apply to download)	225.00	185.00
CDB-10S	CD-ROM—Spanish Edition	225.00	185.00
CDB-10SW	Download—Spanish Edition (No shipping charges apply to download)	225.00	185.00
CAN*	Candidate's Guide to the CISA Exam and Certification 2010 (No charge to paid CISA exam registrants)	15.00	5.00

2010 CISM® EXAM REFERENCE MATERIALS

◆ *To prepare for the **December 2010** CISM exam, order* ◆

CISM Review Manual 2010*			
CM-10	English Edition	115.00	85.00
CM-10J	Japanese Edition	115.00	85.00
CM-10S	Spanish Edition	115.00	85.00
CISM Review Questions, Answers & Explanations Manual 2010 Supplement*			
CQA-10ES	English Edition (100 questions)	60.00	40.00
CQA-10JS	Japanese Edition (100 questions)	60.00	40.00
CQA-10SS	Spanish Edition (100 questions)	60.00	40.00
CISM Review Questions, Answers & Explanations Manual 2009*			
CQA-9	English Edition (450 questions)	90.00	70.00
CQA-9J	Japanese Edition (450 questions)	90.00	70.00
CQA-9S	Spanish Edition (450 questions)	90.00	70.00
CISM Review Questions, Answers & Explanations Manual 2009 Supplement*			
CQA-9ES	English Edition (100 questions)	60.00	40.00
CQA-9JS	Japanese Edition (100 questions)	60.00	40.00
CQA-9SS	Spanish Edition (100 questions)	60.00	40.00
CISM Practice Question Database v10 (650 questions)*			
MDB-10	CD-ROM—English Edition	160.00	120.00
MDB-10W	Download—English Edition (No shipping charges apply to download)	160.00	120.00
CGC*	Candidate's Guide to the CISM Exam and Certification 2010 (No charge to paid CISM exam registrants)	15.00	5.00

2010 CGEIT EXAM REFERENCE MATERIAL

◆ See *www.isaca.org/cgeitreferences* for IT governance resources ◆
to prepare for the December 2010 CGEIT exam.

CGM-10*	CGEIT Review Manual 2010	115.00	85.00
CACG*	Candidate's Guide to the CGEIT Exam and Certification 2010 (No charge to paid CGEIT exam registrants)	15.00	5.00

COBIT®

CB4.1*	COBIT 4.1, Print Format	190.00	75.00
COBIT and Application Controls: A Management Guide			
WCAC*	E-book—PDF format (purchase online only)	55.00	FREE
CAC*	Print format	75.00	35.00
CBX*	COBIT 4.1 Excerpt	5.00	5.00
CPS2*	COBIT Control Practices: Guidance to Achieve Control Objectives for Successful IT Governance, 2nd Edition	110.00	55.00
CBQ2*	COBIT Quickstart, 2nd Edition	110.00	55.00
CBSB2*	COBIT Security Baseline, 2nd Edition	40.00	20.00
	Additional Set (5 each) Reference Cards		
	HRC2 Home Users	3.00	2.00
	PRC2 Professional Users	3.00	2.00
	MRC2 Managers	3.00	2.00
	ERC2 Executives	3.00	2.00
	SRC2 Senior Executives	3.00	2.00
	BRC2 Board of Directors/Trustees	3.00	2.00
COBIT User Guide for Service Managers			
WCUG*	E-book—PDF format (purchase online only)	35.00	FREE
CUG*	Print format	50.00	20.00
CB4A*	IT Assurance Guide: Using COBIT	165.00	55.00
ITG9*	Implementing and Continually Improving IT Governance	115.00	55.00
SDG*	SharePoint Deployment and Governance Using COBIT 4.1: A Practical Approach	70.00	30.00
COBIT Online 4.1			
COLB*	**Annual Full Subscription + Benchmarking (purchase online at *www.isaca.org/cobitonline*) ISACA members SAVE 75%**	**400.00**	~~**200.00**~~ **50.00**

▶ **Visit *www.isaca.org/cobitonline* for additional information.** ◀

COBIT Mappings			
WCMCMM*	Mapping of CMMI for Development V1.2 With COBIT 4.0	25.00	Free
WCMISO*	Mapping of ISO/IEC 17799: 2005 With COBIT 4.0	25.00	Free
WCMIT3*	Mapping of ITIL V3 With COBIT® 4.1	25.00	Free
WCMNIST*	Mapping of NIST SP800-53 Rev 1 With COBIT® 4.1	25.00	Free
WCMPMB*	Mapping of PMBOK to COBIT 4.0	25.00	Free
WCMSEI*	Mapping of SEI's CMM for Software to COBIT 4.0	25.00	Free
WCMTOG*	Mapping of TOGAF 8.1 With COBIT 4.0	40.00	Free
WCMFF*	Mapping FFIEC with COBIT 4.1	25.00	Free

Sets of related COBIT products focusing on your professional needs are available—purchase a focus set and save!
See *www.isaca.org/cobitbooks* for components included in each Focus Set

CBVH	IT Governance Based on COBIT® 4.1: A Management Guide	45.00	35.00

Meycor COBIT Suite
Comprehensive software for implementing COBIT 4.1 as an IT governance, security or assurance tool. (see *www.isaca.org/cobit* for descriptions and pricing)

See **NON-ENGLISH RESOURCES** for additional COBIT material.

VAL IT™

Enterprise Value: Governance of IT Investments			
VITM*	Getting Started With Value Management	40.00	25.00
VITF2*	The Val IT Framework 2.0	90.00	45.00
VITB2*	The Business Case Guide—Using Val IT 2.0	40.00	25.00
VITAG*	Value Management Guidance for Assurance Professionals—Using Val IT 2.0	40.00	25.00
VITS2*	Complete Set	185.00	105.00

RISK IT AND RISK RELATED TOPICS

24-CRC	Assessing and Managing Security Risk in IT Systems: A Structured Methodology	75.00	65.00
78-WRM	The Failure of Risk Management: Why It's Broken and How to Fix It	55.00	45.00
70-WFR	Fraud Risk Assessment: Building a Fraud Audit Program	75.00	65.00
27-CRC	Guide to Optimal Operational Risk and Basel II	115.00	105.00
11-CRC8	How to Complete a Risk Assessment in 5 Days or Less	90.00	80.00
84-WRM	Information Technology Risk Management in Enterprise Environments	100.00	90.00
2-HBS	IT Risk: Turning Business Threats Into Competitive Advantage	45.00	35.00
5-PL	Risk Assessment & Risk Management	105.00	95.00
55-WRCS	Risks, Controls, and Security: Concepts and Applications	111.00	101.00
RITF*	The Risk IT Framework	95.00	45.00
RITPG*	The Risk IT Practitioner Guide	115.00	55.00
5-RO	A Risk Management Approach to Business Continuity: Aligning Business Continuity with Corporate Governance	105.00	95.00

AUDIT, CONTROL AND SECURITY—ESSENTIALS

1-IT8	Accounting Information Systems, 8th Edition	225.00	215.00
70-WAS	Accounting Information Systems: Controls and Processes	155.00	145.00
6-PAW	Applied Security Visualization	65.00	55.00
45-WAP	Audit Planning: A Risk-Based Approach	75.00	65.00
6-PL	Auditing IT Infrastructures	105.00	95.00
53-WAG	Auditor's Guide to Information Systems Auditing	108.00	98.00
7-EL	Biometric Technologies and Verification Systems	79.00	69.00
76-WSL	Build Your Own Security Lab: A Field Guide for Network Testing	60.00	50.00

Shaded — New Books * Published by ISACA and ITGI PRICES SUBJECT TO CHANGE

ISACA Bookstore Price List

Code	Title	Nonmember	Member
43-CRC	Building an Effective Information Security Policy Architecture	90.00	80.00
31-CRC	Complete Guide to Security and Privacy Metrics: Measuring Regulatory Compliance, Operational Resilience and ROI	135.00	125.00
79-WCAF	Computer Aided Fraud Prevention and Detection: A Step by Step Guide	70.00	60.00
4-IGI	Computer Security, Privacy and Politics: Current Issues, Challenges and Solutions	110.00	100.00
30-WCC	Core Concepts of Information Technology Auditing	99.00	89.00
50-WPM5	Effective Project Management: Traditional, Agile, Extreme, 5th Edition	60.00	50.00
Enterprisewide Identity Management			
WIM*	E-book—PDF Format (purchase online only)	20.00	10.00
PIM*	Print Format	35.00	25.00
71-WCF	Essentials of Corporate Fraud	50.00	40.00
60-WESO	Essentials of Sarbanes-Oxley	45.00	35.00
82-WACL	Fraud Analysis Techniques Using ACL	210.00	200.00
62-WFC	Fraud Casebook: Lessons from the Bad Side of Business	80.00	70.00
10-EL	GFI Network Security and PCI Compliance Power Tools	73.00	63.00
68-WHF	Healthcare Fraud: Auditing and Detection Guide	80.00	70.00
36-CRC	How to Achieve 27001 Certification: An Example of Applied Compliance Management	94.00	84.00
2-W404	How to Comply with Sarbanes-Oxley Section 404: Assessing the Effectiveness of Internal Control, 3rd Edition	90.00	80.00
7-ART	Implementing the ISO/IEC 27001 Information Security Management System Standard	95.00	85.00
9-CRC	Information Security Architecture: An Integrated Approach to Security in the Organization, 2nd Edition	94.00	84.00
28-CRC	Information Security: Design, Implementation, Measurement and Compliance	104.00	94.00
83-WIS	Information Storage and Management: Storing, Managing, and Protecting Digital Information	70.00	60.00
4-CRC3	Information Technology Control and Audit, 3rd Edition	100.00	90.00
35-CRC	Insider Computer Fraud: An In-depth Framework for Detecting and Defending Against Insider IT Attacks	94.00	84.00
STDPK*	IT Standards and Summaries of Guidelines and Tools and Techniques for Audit and Assurance and Control Professionals	20.00	15.00
WITAF*	ITAF: A Professional Practices Framework for IT Assurance e-book—PDF (purchase online only)	45.00	FREE
11-PL	IT Auditing: IT Governance	105.00	95.00
8-PL	IT Auditing: The Process	105.00	95.00
15-MIT	IT Auditing: Using Controls to Protect Information Assets	70.00	60.00
IT Control Objectives for Basel II			
WITCOB*	E-book—PDF Format (purchase online only)	35.00	FREE
ITCOB*	Print Format	50.00	20.00
PSOX*	IT Control Objectives for Sarbanes-Oxley: The Role of IT in the Design and Implementation of Internal Control Over Financial Reporting, 2nd Edition	40.00	20.00
9-SYN	The IT Regulatory and Standards Compliance Handbook: How to Survive Information Systems Audit and Assessments	80.00	70.00
5-ART	Outsourcing Information Security	103.00	93.00
7-SYN9	PCI Compliance, Second Edition	70.00	60.00
26-CRC	A Practical Guide to Security Assessments	94.00	84.00
1-RIA	Practical IT Auditing with current Supplement	400.00	390.00
69-WPS	Public Sector Auditing: Is IT Value for Money?	70.00	60.00
8-ART	Role Engineering for Enterprise Security Management	95.00	85.00
75-WSO	The Sarbanes-Oxley Section 404 Implementation Toolkit: Practice Aids for Managers and Auditors, 2nd Edition	95.00	85.00
1-IGI	Securing the Information Infrastructure	110.00	100.00
5-PSM	Security Metrics: Replacing Fear, Uncertainty, and Doubt	60.00	50.00
1-SCC	Spreadsheet Check and Control: 47 Key Practices to Detect and Prevent Errors	50.00	40.00
2-WG	Standard for Auditing Computer Applications	470.00	460.00
2-BAY*	Stepping Through the InfoSec Program	45.00	35.00
1-BAY*	Stepping Through the IS Audit, 2nd Edition	45.00	35.00

AUDIT, CONTROL AND SECURITY—SPECIFIC ENVIRONMENTS

18-MAO	Applied Oracle Security: Developing Secure Database and Middleware Environments	70.00	60.00
4-DC	Audit Guideline for DB2	80.00	70.00
1-SAPP	COBIT and the Sarbanes-Oxley Act	45.00	35.00
Linux: Security, Audit and Control Features			
WLIN*	E-book—PDF Format (purchase online only)	30.00	15.00
PLIN*	Print Format	50.00	35.00
Managing Risk in Wireless Environment: Security, Audit and Control Issues			
WW*	E-book—PDF Format (purchase online only)	40.00	20.00
PW*	Print Format	50.00	35.00
1-IPG	Oracle Privacy Security Auditing	70.00	60.00
OS390*	OS/390-z/OS Security, Audit and Control Features	70.00	55.00
29-ST4	A Practical Guide to IBM i and i5/OS Security and Compliance	89.00	79.00
ODB9*	Security, Audit and Control Features Oracle® Database, 3rd Edition	55.00	40.00
ISOA3*	Security, Audit and Control Features Oracle® E-Business Suite, 3rd Edition	75.00	60.00
ISPS*	Security, Audit and Control Features PeopleSoft®, 2nd Edition	70.00	55.00
ISAP3*	Security, Audit and Control Features SAP® ERP, 3rd Edition	75.00	60.00
3-EL	Wireless Operational Security	91.00	81.00

NON-ENGLISH RESOURCES

3-RAMA	Auditoría de Tecnologías y Sistemas de Información	70.00	60.00

CISA Examination Reference Material
Study aids available in French, Italian, Japanese and Spanish for the December 2010 CISA exam—see page S1

CISM Examination Reference Material
Study aids available in Japanese and Spanish for the December 2010 CISM exam—see page S1

COBIT 3rd Edition, available at the following web site
Korean Edition—*www.isaca.or.kr*

COBIT 4.0 Edition, available at the following web sites
German Edition—*www.isaca.at*
Italian Edition—*www.aiea.it*

COBIT 4.1 Edition, available at the following web site
French Edition—*www.afai.fr*
Japanese Edition—*www.isaca.gr.jp*
Hungarian Edition—*www.isaca.hu*
Portuguese Edition—*www.isaca.org/downloads*
Russian Edition—*www.isaca-russia.ru*
Spanish Edition—*www.isaca.org/downloads*

1-AOCF	Computación Forense: Descubriendo los Rastros Informáticos	42.00	32.00
2-RAMA	Gobierno de las Tecnologías y los Sistemas de Información	65.00	55.00

Meycor COBIT Suite
Meycor COBIT es un software completo e integrado para la implementación de COBIT como una herramienta para el Buen Gobierno de la TI, Seguridad de la TI o Aseguramiento de la TI según COBIT 4.1. (see *www.isaca.org/nonenglishbooks* para descripción y precios)

ISOAJ*	Security, Audit and Control Features Oracle E-Business Suite: A Technical and Risk Management Reference Guide—(Japanese Version)	70.00	55.00
ISAPJ*	Security, Audit and Control Features SAP R/3: A Technical and Risk Management Reference Guide—(Japanese Version)	70.00	55.00

INTERNET AND RELATED SECURITY TOPICS

19-M24	24 Deadly Sins of Software Security: Programming Flaws and How to Fix Them	60.00	50.00
7-MOA3	Anti-Hacker Toolkit, 3rd Edition	70.00	60.00
37-WAI	The Art of Intrusion: The Real Stories Behind the Exploits of Hackers, Intruders & Deceivers	27.00	17.00
1-NBS	The Big Switch: Rewiring the World, from Edison to Google	27.00	17.00
45-CRC	Cloud Computing: Implementation, Management, and Security	90.00	80.00
10-MOC	The Complete Reference Network Security	73.00	63.00
9-EL	Computer and Information Security Handbook	130.00	120.00
Cybercrime: Incident Response and Digital Forensics			
WCC*	E-book—PDF Format (purchase online only)	45.00	25.00
PCC*	Print Format	55.00	40.00
1-CAP	Cybercrime: The Investigation, Prosecution and Defense of a Computer-Related Crime, 2nd Edition	47.00	37.00
34-CRC	Cyber Forensics: A Field Manual for Collecting, Examining, and Preserving Evidence of Computer Crimes, 2nd Edition	84.00	74.00
4-MGH	Gray Hat Hacking, 2nd Edition	60.00	50.00
1-MHF	Hacking Exposed Computer Forensics Secrets and Solutions, 2nd Edition	60.00	50.00
2-MCG6	Hacking Exposed: Network Security Secrets & Solutions, 6th Edition	60.00	50.00
8-SYN	How to Cheat at Configuring Open Source Security Tools	60.00	50.00
29ST-3	The Little Black Book of Computer Security, 2nd Edition	35.00	25.00
86-WNS	Network Security Bible, 2nd Edition	70.00	60.00
59-WNS	Network Security Fundamentals	74.00	64.00
1-GL	NMAP Network Scanning: The Official NMAP Project Guide to Network Discovery and Security Scanning	60.00	50.00
56-WPC	Phishing and Countermeasures: Understanding the Increasing Problem of Electronic Identity Theft	100.00	90.00
1-HA	Scrappy Information Security: The Easy Way to Keep the Cyber Wolves at Bay	30.00	20.00
30-CRC	Securing Converged IP Networks	90.00	80.00
1-OSM	Security Monitoring	55.00	45.00
6-EL	XSS Exploits—Cross Site Scripting Attacks and Defense	70.00	60.00

Shaded — New Books * Published by ISACA and ITGI PRICES SUBJECT TO CHANGE

ISACA Bookstore Price List

IT GOVERNANCE AND BUSINESS MANAGEMENT

Code	Title	Nonmember	Member
3-PAGE	7 Steps to Better Written Policies and Procedures	30.00	20.00
2-PAGE	Achieving 100% Compliance of Policies and Protection	50.00	40.00
8-EL	Architecture and Patterns for IT Service Management, Resource Planning, and Governance: Making Shoes for the Cobbler's Children	57.00	47.00
1-RO	Auditing Business Continuity: Global Best Practices	99.00	89.00
61-WBSC	Balanced Scorecard Step-by-Step: Maximizing Performance and Maintaining Results, 2nd Edition	55.00	45.00
4-PAGE	Best Practices in Policies and Procedures	36.00	26.00
1-ITG*	Board Briefing on IT Governance, 2nd Edition	7.00	7.00
66-WCP	Building a World-Class Compliance Program: Best Practices and Strategies for Success	55.00	45.00
6-SYN	Business Continuity and Disaster Recovery Planning for IT Professionals	70.00	60.00
4-RO	Business Continuity Planning: A Step-by-Step Guide With Planning Forms on CD-ROM, 3rd Edition	109.00	99.00
41-CRC	Business Resumption Planning, 2nd Edition	100.00	90.00
39-CRC	The Business Value of IT: Managing Risks, Optimizing Performance and Measuring Results	84.00	74.00
54-WCIO	CIO Best Practices: Enabling Strategic Value with Information Technology	70.00	60.00
38-CRC	CISO Leadership: Essential Principles for Success	84.00	74.00
47-WCG	Corporate Governance Best Practices: Strategies for Public, Private and Not-for-Profit Organizations	70.00	60.00
74-WCM	Corporate Management, Governance, and Ethics Best Practices	75.00	65.00
32-CRC	Crisis Management Planning and Execution	85.00	75.00
1-WBC	The Definitive Handbook of Business Continuity Management, 2nd Edition	85.00	75.00
37-CRC	Digital Privacy: Theory, Technologies, and Practices	84.00	74.00
2-IGI	Emerging Topics and Technologies in Information Systems	205.00	195.00
39-WED	Enterprise Dashboards: Design and Best Practices for IT	55.00	45.00
9-ART	Enterprise Information Security and Privacy	109.00	99.00
1-CMP	Enterprise Security Architecture: A Business-Driven Approach	93.00	83.00
1-PAGE	Establishing a System of Policies and Procedures	36.00	26.00
23-WIT	The Executive's Guide to Information Technology, 2nd Edition	95.00	85.00
10-VH	Foundations of IT Service Management Based on ITIL® V3	76.00	66.00
3-VH	Frameworks for IT Management	76.00	66.00
85-WF101	Fraud 101: Techniques and Strategies for Understanding Fraud, 3rd Edition	60.00	50.00
72-WGP	Global Perspectives in Information Security: Legal, Social, and International Issues	80.00	70.00
64-WGRC	Governance, Risk and Compliance Handbook: Technology, Finance, Environmental, and International Guidance and Best Practices	155.00	145.00
42-CRC	The Green and Virtual Data Center	90.00	80.00
20-MHE	Hacking Exposed Malware and Rootkits: Malware & Rootkits Secrets & Solutions	60.00	50.00
63-WHM	How to Measure Anything: Finding the Value of Intangibles in Business	55.00	45.00
67-WHF	Human Factors in Project Management: Concepts, Tools, and Techniques for Inspiring Teamwork and Motivation	60.00	50.00
WGOALS*	Identifying and Aligning Business Goals and IT Goals (E-book—PDF purchase online only)	35.00	20.00
4-ID	Implementing Information Technology Governance: Models, Practices and Cases	110.00	100.00
7-VH	Implementing IT Governance: A Practical Guide to Global Best Practices in IT Management	76.00	66.00
2-ITG*	Information Security Governance: Guidance for Boards of Directors and Executive Management, 2nd Edition	7.00	7.00
	Information Security Governance: Guidance for Information Security Governance:		
3-ITG*	Information Security Governance: Guidance for Information Security Managers	50.00	25.00
W3ITG*	E-book—PDF Format (purchase online only)	45.00	FREE
43-WSA	Information Security: A Strategic Approach	79.00	69.00
WSH*	Information Security Harmonisation: Classification of Global Guidance (E-book—PDF format purchase online only)	40.00	FREE
1-BS	Information Security Policies Made Easy, Version 11	805.00	795.00
8-CRC	Information Security Policies and Procedures: A Practitioner's Reference, 2nd Edition	104.00	94.00
2-PS	Information Security Roles & Responsibilities Made Easy, Version 2	505.00	495.00
65-WISM	Information Systems for Managers: Text and Cases	134.00	124.00
3-ID	Information Technology Ethics: Cultural Perspectives	175.00	165.00
3-IGI	Information Technology Governance and Service Management: Frameworks and Adaptations	205.00	195.00
80-WITM	Information Technology for Management: Improving Performance in the Digital Economy, 7th Edition	197.00	187.00
81-WIC	Internal Controls Policies and Procedures	85.00	75.00
4-VH	ISO 9001:2000 The Quality Management Process	76.00	66.00
5-VH	ISO/IEC 20000: A Pocket Guide	35.00	25.00
12-VH	IT Financial Management	76.00	66.00
ITGS8*	IT Governance Global Status Report 2008	55.00	40.00
5-AS10	IT Governance: Policies & Procedures 2010 Edition	219.00	209.00
WGPM*	IT Governance and Process Maturity (E-Book—purchase online only)	30.00	FREE
11-VH	IT Outsourcing: Part 1 Contracting the Partner	50.00	40.00
6-ART	IT Project Portfolio Management	99.00	89.00
8-VH	IT Service Management Global Best Practices	120.00	110.00
40-CRC	Leading IT Projects: The IT Manager's Guide	90.00	80.00
49-WMG	Manager's Guide to Compliance: Best Practices and Case Studies	75.00	65.00
	Managing Enterprise Information Integrity: Security, Control and Audit Issues		
WME*	E-book—PDF Format (purchase online only)	45.00	25.00
PME*	Print Format	55.00	40.00
9-VH	MOF—Microsoft Operations Framework V4.0: A Pocket Guide	35.00	25.00
2-ITO	Outsourcing IT: A Governance Guide	82.00	72.00
6-RO	Principles and Practice of Business Continuity: Tools and Techniques	109.00	99.00
1-IS	The Privacy Management Toolkit	505.00	495.00
1-HBS	Reinventing Project Management: The Diamond Approach to Successful Growth and Innovation	45.00	35.00
5-SYN	Sarbanes-Oxley IT Compliance Using Open Source Tools, 2nd Edition	70.00	60.00
	Security Awareness: Best Practices to Secure Your Enterprise		
WSA*	E-book—PDF Format (purchase online only)	35.00	20.00
PSA*	Print Format	50.00	35.00
58-WSOA	Service Oriented Architecture: A Planning and Implementation Guide for Business and Technology	70.00	60.00
73-WSOA	Service Oriented Architecture Field Guide for Executives	60.00	50.00
6-VH	Six Sigma for IT Management	76.00	66.00
5-ID	Social and Human Elements of Information Security: Emerging Trends and Countermeasures	205.00	195.00
77-WTS	Technology Scorecards: Aligning IT Investments with With Business Performance	60.00	50.00
4-ITG*	Unlocking Value: An Executive Primer on the Critical Role of IT Governance	7.00	7.00
2-ITPI	Visible OPS Security: Achieving Common Security and IT Operations Objectives in 4 Practical Steps	32.00	22.00
1-ITPI	The Visible Ops: Starting ITIL in 4 Practical Steps	32.00	22.00
44-CRC	Vulnerability Management	90.00	80.00
1-EA	Winning as a CISO	30.00	20.00

Shaded — New Books * Published by ISACA and ITGI PRICES SUBJECT TO CHANGE

FOUR EASY WAYS TO PLACE AN ORDER:

Online
Order online at
www.isaca.org/bookstore

BankWires:
Send electronic payments in US dollars to:
Bank of America, ABA #0260-0959-3
ISACA Account #22-71578
S.W.I.F.T code BOFAUS3N

Mail
Mail completed form with payment:
ISACA/ITGI
1055 Paysphere Circle
Chicago, IL 60674-1055 USA

Fax
Fax completed order form with credit card number and expiration date to +1.847.253.1443

RETURN POLICY

All purchases are final. No refunds or exchanges.

PUBLICATION QUANTITY DISCOUNTS

Academic and bulk discounts are available on books published by the ISACA and IT Governance Institute. Please call +1.847.660.5501 or +1.847.660.5578 for pricing information.

Phone
+1.847.660.5650
Monday-Friday, 8:00 am-5:00 pm Central Time (Chicago, Illinois, USA) Personal service—please have credit card number available. We will confirm availability and expected delivery date.

ISACA® Customer Order Form

Trust in, and value from, information systems

OFFICE USE ONLY

Vol. 5 -10

PLEASE NOTE: READ PAYMENT TERMS AND SHIPPING INFORMATION BELOW. ALL ORDERS MUST BE PREPAID.

Please return to: ISACA, 1055 Paysphere Circle, Chicago, IL 60674, USA
Phone: +1.847.660.5650 Fax: +1.847.253.1443 E-mail: *bookstore@isaca.org*

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

Date_____

Customer Information

Name _____
FIRST MIDDLE LAST/FAMILY

ISACA Member: ☐ No ☐ Yes Member Number _____

Company Name _____

Address: ☐ Home ☐ Company

_____

_____

City _____ State/Province_____

Country_____ Zip/Mail Code_____

Phone Number ( ) _____

Fax Number ( ) _____

E-mail Address _____

Shipping Information (If different from customer information)

If shipping to a PO Box, please include street address to ensure proper delivery.

Name _____
FIRST MIDDLE LAST/FAMILY

Company Name _____
(IF PART OF SHIPPING ADDRESS)

Address: _____

_____

_____

City _____ State/Province_____

Country_____ Zip/Mail Code_____

Phone Number ( ) _____

E-mail Address _____

Code	Title/Item	Quantity	Unit Price	Total

Thank you for ordering from ISACA. **All purchases are final.**

Subtotal	
Sales Tax: Add sales tax if shipping to: Louisiana (LA), Oklahoma (OK)—4%	
Wisconsin (WI)—5%	
Florida (FL), Minnesota (MN), Pennsylvania (PA), South Carolina (SC), Texas (TX), Washington (WA)—6%	
New Jersey (NJ), Tennessee (TN)—7%	
California (CA)—8%	
Illinois (IL)—9%	
For all orders please include shipping and handling charge—see chart below.	
TOTAL	

Payment Information—Prepayment Required

☐ Payment enclosed. Check must be payable in US dollars, drawn on US bank and made payable to ISACA.

☐ Bank wire transfer in US dollars. Date of transfer _____

☐ Charge to ☐ Visa ☐ MasterCard ☐ American Express ☐ Diners Club

Account # _____

Exp. Date_____

Print Cardholder Name _____

Signature of Cardholder_____

Cardholder Billing Address (if different than above)_____

_____

_____

Shipping details *www.isaca.org/shipping*
International customers are solely responsible for paying all custom duties, service charges, and taxes levied by their country.

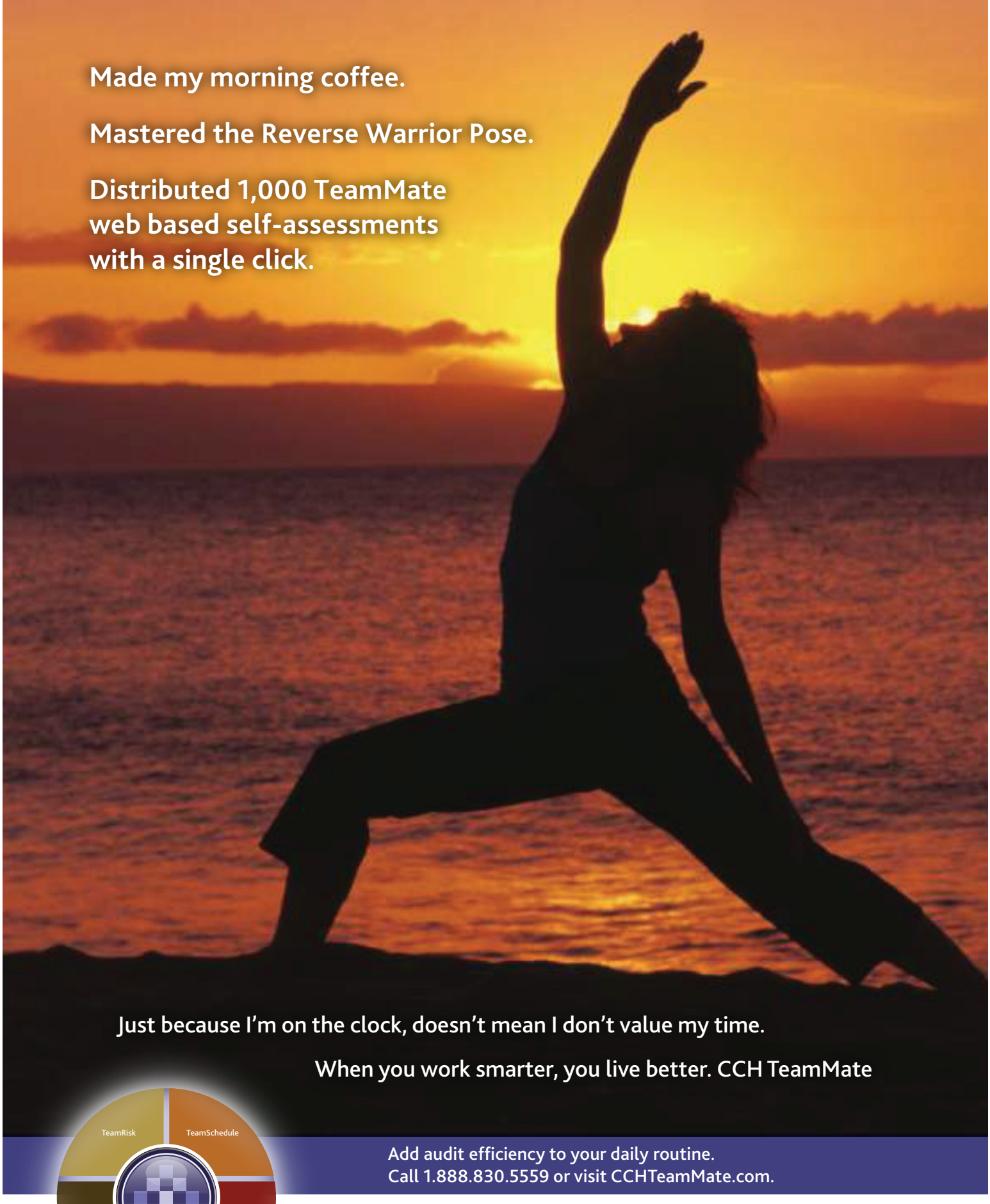
All purchases are final. **Pricing, shipping and handling, and tax are subject to change without notice.**

Shipping & Handling Rates for Orders

All orders outside the US are shipped Federal Express Priority.

For Orders Totaling	Outside US	Within US
Up to US $30.00	US $10.00	US $5.00
US $30.01 to US $50.00	US $15.00	US $7.00
US $50.01 to US $80.00	US $20.00	US $8.00
US $80.01 to US $150.00	US $26.00	US $10.00
Over US $150.00	17% of Total	10% of Total

No shipping charges apply to *Meycor COBIT*.
No shipping charges apply to CISA Practice Question Database v10—download.
No shipping charges apply to CISM Practice Question Database v10—download.


Made my morning coffee.
Mastered the Reverse Warrior Pose.
Distributed 1,000 TeamMate web based self-assessments with a single click.
Just because I'm on the clock, doesn't mean I don't value my time.
When you work smarter, you live better. CCH TeamMate
TeamRisk
TeamSchedule
TeamCentral
TeamMate TEC
TeamMate EWP
Add audit efficiency to your daily routine.
Call 1.888.830.5559 or visit CCHTeamMate.com.
CCH® TeamMate
Audit Management System
ARC Logics™
a Wolters Kluwer business
GRC-10-1368

BALANCE

Risk with Reward

CRISC™ Certified in Risk and Information Systems Control™
An ISACA® Certification

Earn ISACA's Certified in Risk and Information Systems Control™ (CRISC™) designation and gain the rewards of recognition and career advancement. Apply for grandfathering today.

Early-bird application deadline 31 October 2010. ***(Save $100)***

www.isaca.org/crisc

The right balance for your career.

ISACA®
Trust in, and value from, information systems