VOLUME 2, 2011

ISACA® Journal

Risk Management — What Is Your Capacity?

Featured articles:

IT Scenario Analysis in Enterprise Risk Management

Key Consideration When Evaluating ISRM Programs and Capabilities

A Cost-effective Approach for Sarbanes-Oxley-regulated Application Systems With Minimal IT Control Assurance

And more...

ISACA®
Trust in, and value from, information systems

WWW.ISACA.ORG

CISA Certified Information Systems Auditor™ An ISACA® Certification

CISM Certified Information Security Manager™ An ISACA® Certification

CGEIT Certified in the Governance of Enterprise IT™ An ISACA® Certification

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

Recognition • Success • Growth

June Exam Date: 11 June 2011
Registration Deadline: 6 April 2011

ISACA®
Trust in, and value from, information systems

SAINT® for Mac OS X

Integrated Vulnerability Scanning, Penetration Testing, and Checklist (Benchmark) Compliance.

Vulnerability Scanning

Assess any target with an IPv4, IPv6, or URL with pre-defined policies for PCI, HIPAA, FISMA, and more.

Identify CVE, OSVDB, IAVA, OVAL, and more.

Penetration Testing

Exploit vulnerabilities to gain remote access.

Run social engineering, phishing assessments, and more with the exploit tools suiite.

Checklist Compliance

Show compliance with FDCC & USGCB security configuration policies defined by NIST SP 800-70.

For more information–

www.saintcorporation.com/mac

1-800-596-2006

SAINT is SCAP validated by NIST & a certified PCI ASV scanning vendor

Copyright © 2011. SAINT Corporation. All Rights Reserved

Volume 2, 2011

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.

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.

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 April 2011.

El Debido Cuidado en Seguridad de la Información
Jeimy J. Cano M. , Ph.D., CFC, CFE, CMAS

Mapping PCI DSS v2.0 With COBIT 4.1
Pritam Bankar, CISA, CISM, and Sharad Verma

The Prevalence of Information Security Controls: Perspectives From IT Auditors
Hui Lin, Ph.D., Meghann Abell Cefaratti, Ph.D., and Linda Wallace, Ph.D.

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

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

Your Comprehensive Resource for Professional Knowledge

ISACA®
Trust in, and value from, information systems

ISACA Bookstore

Get the latest in peer-reviewed publications, reference materials and certification review materials to support your professional development.

Visit *www.isaca.org/bookstore*

What Is the Value of Security?

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

The question in the title is not an idle one, meant to be answered: "Oh, certainly, security is very valuable." Rather, it is a challenge to those concerned with information security to place a monetary value on the protection of information resources. In every organization in which the need for information security is recognized, there is an expenditure to protect information and the systems that manage it against natural, technical and man-made hazards. What does an organization gain by the money it pays for security? This is more than the return on security investment (ROSI),[1] which deals with the payback for individual outlays for equipment, software and services that safeguard information. The question is how much more is a secure company worth than an insecure one?

SECURE AND INSECURE

The terms "secure" and "insecure" are very much open to interpretation. What makes an organization demonstrably *insecure*? Fraud? Data leakage? Privacy violations? Does the absence of those things make an organization secure? If absolute terms are avoided, we can say that some industries need and have a higher level of security than others, and that organizations within those industries also differ in the level of security they have attained. Even this is definitional; some may have better access control while others make better use of encryption or have more effective business continuity plans. But, however defined or interpreted, each organization is secured to a certain extent that differs from the other. In that case, how much value does greater security add to a company or government agency as compared with its peers or against some absolute metric?

Is that the way security is viewed by the management of most organizations? I fear not. In many instances, security is, at worst, viewed as an annoying inconvenience best circumvented. More positively, security may be a response to regulation or perceived risk. In my experience, security is rarely perceived as a competitive advantage, and I am aware of no cases in which a financial value is placed on it. Management does not think of security that way, largely because security professionals do not make the business case for security in that manner. It is time to change that perspective.

To do so, I propose a simple thought experiment. A company has annual earnings of 1 billion (the currency is irrelevant, so long as this comes out to be a fairly large number). It has market capitalization of 6 billion. A potential buyer offers between 6 and 9 billion for the company, to be determined after a due-diligence review of its financial statements and internal controls. Assuming that the company's books are materially correct, how much less than 9 billion would the business be worth if security were shown to be inadequate?

THRESHOLD CONDITION

One view is that security would be a threshold condition for such a sale. If security did not meet some basic set of expectations, there would be no acquisition at all. Insecurity would raise questions about the stability of the business and its ability to sustain itself over the long term. The absence, or near absence, of even rudimentary security would indicate a management that is blind to potential risks. What, then, is basic security or a baseline set of controls? Exercising due diligence, one would expect to find at least a security policy supported by standards, access controls, privacy protection and some form of recoverability, especially for electronic data.

Is this a definition of "adequacy"? A C- is a passing grade, but it is hardly indicative of mastery of a subject. Still, the potential buyer of the imaginary company might accept that the *necessary* security was present, while using the degree of it to justify the acquisition at a lower price. I once sat across the table from a man who would make millions that very afternoon if I merely stated that my review indicated adequate, if not particularly advanced, security in the company he was about to sell. He was able to place a very clear value on security at that moment.

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.

SUFFICIENT SECURITY

Another way to measure the value of security is based on the concept of *sufficiency*. The term sufficiency raises the question of some independent metric on which to base a decision. Such metrics exist in regulated industries and are often implicit in others. It is important to realize that appropriate security goes beyond adequacy; the adequate level is necessary but not sufficient. Thus, for example, the controls required to enforce separation of duties may be considered acceptable for financial systems, but not enough for trades over a billion or for access to trade secrets and proprietary formulas. Thus, if merely adequate security would enable completion of the acquisition at 6 billion, sufficient security would raise the price higher. How much higher is a matter of negotiation, but in terms of establishing value, sufficiency does raise the ante.

Sufficiency as a concept, or perhaps only as a term, has its dangers. If security is sufficient at a certain level, there is no incentive for more of it, regardless of risk. Placing a value on "just enough" security bases it on average circumstances. It ignores the possibility that security might prove insufficient in extreme but nonetheless predictable situations, thereby wiping out value all at once. I would, therefore, suggest that any definition of "sufficient security" include risk management processes.

INTELLECTUAL PROPERTY

The value of an organization's intellectual property is tied to that of its information security. "A formal valuation of intellectual property most likely will refer to a standard of fair market value. This is the standard of value to which the analysis and all assumptions necessary in the valuation exercise have been held. It differs in some very important aspects from a strict calculation of the benefits derived from using the [intellectual property]."[2] Thus, if intellectual property adds quantifiable value depending on its worth in the marketplace (very much like the thought experiment), it is wholly dependent on information security to retain that value.

The techniques for assessing value of intellectual property include a cost approach and the aggregate expenditure to develop it. Therefore, it follows that the cost of securing intellectual property is at least a part of the added value that security brings to an organization. A market approach places a value on intellectual property based on what it would bring if sold.

This actually shows up on balance sheets as "goodwill and other intangible assets."[3] Even if security were viewed as only a percentage of the overall value of intellectual property, it would be possible to place a monetary figure on it.

PERCENTAGE OF SALES

Finally, the value of security can be determined by the income derived from it. In commercial companies, this means sales revenue, which can be shown to be tied in some instances to security. This is not just theory. In the past, I assisted a client who needed to choose between two highly respected vendors for the same service. They were equivalent in terms of effectiveness, responsiveness, financial stability and fees. I was asked to evaluate them in terms of security; one was clearly superior, especially with regard to recoverability. That company received a very lucrative contract, which added to its bottom line.

It would be foolish to attribute the value of all sales to security, but it would be equally silly to disregard it as a factor. Once again, the monetary amount is negotiable. As a part of the thought experiment, one might say that 10 percent of all sales would be lost if security were not present, or at least not sufficient for the marketplace. Security, therefore, represents 100 million in annual revenue and would add at least 600 million to the acquisition price.

The purpose of this discourse into the value of security is to challenge the idea that it is simply a cost to an organization. Security professionals should state the worth of their contribution in monetary terms to establish the rationale for their activities in the same terms that profit centers do. This will provide not only a basis for managing the appropriate level of security for an organization, but will also demonstrate how much value is lost by not having enough security.

ENDNOTES

[1] See Ross, Steven; "ROSI Scenarios," *Information Systems Control Journal*, vol. 3, 2002. When I began writing on the subject, there was not much literature about it. Today, an Internet search on "return on security investment" brings 8,900,000 references.

[2] Drews, David; "Intellectual Property Valuation Techniques," IPMetrics, *www.ipmetrics.net/IPVT.pdf*

[3] *Ibid.*, p. 4–6. This is terminology from the US Financial Accounting Standard 142, of the same name.

IT Audit Basics

Understanding the New SOC Reports

Tommie W. Singleton, Ph.D., CISA, CGEIT, 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*.

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.

With the transition from Statement on Auditing Standard (SAS) No. 70 reports to the new Service Organization Controls (SOC) reports, this issue's column describes these reports to provide an understanding of them, and to explain the differences among them in order to prepare CISAs for the changes ahead.

SAS 70 AND THE NEED FOR SOC

About 18 years ago, the American Institute of Certified Public Accountants (AICPA) adopted SAS 70, "Service Organizations."[1] The purpose of a SAS 70 audit was (and is) to gather evidence on internal controls of a service organization (SO) in which those controls were associated with the delivery of a service that was (and is) related to the financial reports and impacted the financial statement to a material degree. Obviously, it was put in place because the financial auditors of the user entity needed to have sufficient assurance on controls over accounts, transactions or disclosures that were material, and some of those events occurred at an SO.[2]

It was not feasible for the user auditors to be able to properly evaluate them on the site of the SO. Thus, there was a need for some assurance over the controls of the SO that are relevant to the financial audit of the service user to be provided by someone other than the user auditor. SAS 70 addressed this by creating an audit of the controls at SOs, to be performed by auditors (i.e., certified public accountants [CPAs]) who were not the user's auditors, and a report written on the results of that audit.[3] The user auditors could then rely on the opinion of the auditor's report to best fulfill their obligations—at a minimum, from an efficiency and effectiveness perspective.

Because many of these services were IT-related or involved IT (e.g., transmission of data or funds electronically), and because of the expansion of the number of controls embedded in IT, Certified Information Systems Auditors (CISAs) were often called on to be a part of the service auditor team. Over these 18 years, CISAs have become more and more involved with SAS 70 audits.

The business community began to appreciate and value a SAS 70 audit even beyond the needs of the user's auditors. For instance, service providers (especially entities such as data centers, cloud computing companies, flexible spending account vendors, banks and retirement account vendors) found that when they called on prospects, the primary concern was one of security (i.e., controls). Thus, a SAS 70 became a valuable marketing tool to show businesses that the user had sufficient controls about which the prospect could be comfortable and could gain an adequate assurance of the level of security being provided. This worked so well that companies began to use a SAS 70 for all sorts of controls assurance for an SO (e.g., a hospital outsources its pharmacy and wants assurance over privacy for US Health Insurance Portability and Accountability Act [HIPAA] purposes). However, SAS 70 specifically stated that it was for internal controls over financial reporting (ICFR) and, thus, not correctly applied to privacy or security audits.

Another issue with SAS 70 audits was that there was no standard set of controls. Instead, management of each SO determined the controls to be evaluated, and thus, there was the possibility that management might not have been able to identify one or more critical controls and, thereby, could have unintentionally tainted the SAS 70 report. Even the identification of controls was not formalized in writing.

THE NEW SERVICE ORGANIZATION CONTROLS REPORTS: SOC-1, SOC-2, SOC-3

Recently, the AICPA addressed these evolving issues about SAS 70 and provided a more effective framework for providing assurance of controls in a service organization.[4] Because of the evolving needs for a variety of the objectives of these controls, AICPA came up with Service Organization Controls (SOC) reports, identified simply as SOC-1, SOC-2 and SOC-3 (see **figure 1** for a summary of the SOC framework). These are based on technical standards of Statement on Standards for Attestation Engagements (SSAE) No. 16 and Trust Services,[5] both adopted in 2010. SOC-1 is related *only* to ICFR, SOC-2 is related to controls over security/systems and privacy, and SOC-3 is related to controls over the same.[6] In addition, AICPA has issued a "clarified SAS 70" that applies to the user auditor only.

Figure 1—SOC Framework			
Applicable…	**SOC-1**	**SOC-2**	**SOC-3**
Standard	SSAE 16: AICPA Guide (2011)	AT 101: AICPA Guide (2011)	AT 101: Technical Practice Aid
Controls	ICFR	Security/ Systems, Privacy	Security/ Systems, Privacy
Controls reference	Undefined	Trust Services Principles[7]/ GAPP[8]	Trust Services Principles/ GAPP
Usage of report	User auditor, management of SO, management of user	Knowledgeable parties (see AT 101)	Anyone

SOC-1: REPORTING ON CONTROLS AT A SERVICE ORGANIZATION

SOC-1 is the report of the service auditor over ICFR and is associated with a new standard that partially replaces the service auditor side of SAS 70. SSAE 16,[9] virtually identical to its international complement, the International Accounting Standards Board (IASB)'s International Standard on Assurance Engagements (ISAE) 3402, provides new guidance for assurance over ICFR in an SO. Both standards become effective for reports on or after 15 June 2011. It is important that CISAs and IT auditors in general understand the differences between SAS 70 and SSAE 16.

SAS 70 vs. SSAE 16

There are a number of differences between SAS 70 and the new SSAE 16, some of which are rather significant—at least to the process of conducting the attest service (see **figure 2**).

Figure 2—SAS 70 vs. SSAE 16[10]		
Issue	**SAS 70**	**SSAE 16**
Focus	ICFR	ICFR (not technically different)
Basis	Management's choice	Risk basis for controls implemented/chosen
Period	Specific point in time: close	System description covers entire period of testing
Assertion	Audit	Attest
Management	Not applicable	Management's written assertion
Use	Basically, the public	User auditor, management of SO, management of user

The focus of both SAS 70 and SSAE 16 is on the ICFR of the user where some controls located at the SO are key controls. That said, some past SAS 70 audits addressed examinations of controls over subject matter other than financial reporting. SSAE 16 cannot be used legitimately to address these other controls, but they can be addressed in SOC-2 and SOC-3 (AT 101). Therefore, there is no difference between the two regarding focus, but in practicality, it may be better to restrict the use of SSAE 16 to ICFR.

Under the old SAS 70, the basis of controls evaluated was the prerogative of the SO's management. Management simply decided which controls to test and, as mentioned previously, sometimes was unable to properly identify key controls. There was no accountability or feedback to management about its choice because the auditors were forbidden from choosing them. In the new standard, management has to identify the risks associated with the service and financial reporting by the user and then identify controls that can mitigate those risks. The clarified SAS 70 provides for the user auditor to evaluate the proper choice of controls.

The period of the controls included in the report was simply a point in time in the old SAS 70. Under SSAE 16, the report covers the entire period of testing used in the report. This fact changes the service auditor's service/process considerably, in planning, testing and gathering evidence.

An obvious difference for the service auditor is the change from audit to attest. AICPA states that audit services are reserved for financial audit, and thus, what the service auditor does is attest. As such, the new standard was issued as an SSAE, applied under AT 101. Attest services are very definitive; management identifies specific procedures and the auditor then performs exactly those procedures (agreed-upon procedures [AUPs]). This approach fits the evaluation of controls for an SO.

A new requirement, among others, is that management must provide a written assertion about the fairness of the presentation of the description of the system and the suitability of the design (type I) and effectiveness (type II) of the controls. The written assertion is part of the final report by the service auditor.

One other noteworthy difference is the users of the report. SAS 70 was designed for multiple users and basically went into the public domain. For instance, many large companies would post their SAS 70 on their web site as a "seal of approval." SOC-1/SSAE 16 restricts use of the report to service/user management and user auditors; that is, it *cannot* be used as a marketing tool to prospects.

Enjoying this article?

- Read the ISACA white paper *New Service Auditor Standard: Service Entity Perspective*

www.isaca.org/research

SOC-2: REPORT ON CONTROLS AT A SERVICE ORGANIZATION RELEVANT TO SECURITY, AVAILABILITY, PROCESSING INTEGRITY, CONFIDENTIALITY OR PRIVACY

This report type is intended to meet the need to understand an SO's internal controls related to such criteria as confidentiality, availability, processing integrity (the conventional information security triangle), security and privacy. The process of performing the attest follows the AICPA guide *Reports on Controls at a Service Organization Over Security, Availability, Processing Integrity, Confidentiality or Privacy* (to be issued in 2011). It is intended for use by stakeholders such as customers, regulators, business partners, suppliers and directors. Similar to SOC-1, there are two types: type I, report on management's description of a service organization's system and the suitability of the design of controls, and type II, report on management's description of an SO's system and the suitability of the design and effectiveness of controls. The reports are restricted in use (see **figure 1**).

SOC-2 should be of great interest to many SOs, including data centers and cloud computing companies. It also applies to any entity subject to HIPAA or the US Gramm-Leach-Bliley Act (GLBA), if nothing else to give owner-managers or board members assurance that they are in compliance with regulations. Banks could also use SOC-2 reports.

SOC-3: TRUST SERVICES REPORT FOR SERVICE ORGANIZATION

Trust Services was revised by AICPA in 2010 to incorporate the former SysTrust (security, etc., of a system) and Privacy (especially personal data) principle documents that were in place for years. This report type is intended to meet the needs of users who want assurance on the controls at an SO such as confidentiality, availability, processing integrity (again, the conventional information security triangle), security and privacy, but who do not have the need for or the knowledge necessary to make effective use of a SOC-2 report. The report is prepared using the AICPA/Canadian Institute of Chartered Accountants (CICA) Trust Services principles.[11] The reports are for general use and, therefore, can be freely distributed or posted on a web site. In fact, it is the only SOC report available to the public. Thus, if an SO wants to have an assurance service and use the subsequent report as a marketing tool, then, by default, the proper report is a SOC-3.

CONCLUSION

These new standards and SOC reports will provide the opportunity for IT auditors, especially CISAs, to perform needed services. IT auditors need to understand these reports, the standards and guidelines behind them, and the differences among them to provide the right service in the proper manner.

Because the controls of these SOC reports are so often embedded in IT, IT auditors, especially CISAs, will be needed to perform the attest services.

ENDNOTES

[1] See AU324 of the American Institute of Certified Public Accountants (AICPA) auditing standards for details of SAS 70.

[2] The user auditors had the option of changing the nature, timing or extent (most likely the latter) in place of examination of controls at the SO. However, there would be a need to do a lot of substantive procedures, and all would likely be manual procedures, which would be an expensive option.

[3] There are two types of SAS 70 reports: Type I (focused on fairness of controls put into place and suitability of the design of the controls) and Type II (same as Type I plus operating effectiveness of the controls). This article focuses on Type II.

[4] For more on SOC reports, visit the AICPA SOC site at *www.aicpa.org/soc*.

[5] Trust Services was changed in 2010 to include the previous SysTrust and Privacy services that have been around for years. The AICPA intends to release a new guide on Trust Services (SOC-2 and SOC-3) in 2011.

[6] SOC-2 differs from SOC-3 primarily in its distribution and the fact that no description of the SO system is required in a SOC-3 report.

[7] AICPA, Trust Services Principles, *www.aicpa.org/trustservices*

[8] AICPA, Generally Accepted Privacy Principles, *www.aicpa.org/privacy*.

[9] AICPA, *Reporting on Controls at a Service Organization*, SSAE 16, 2010

[10] There are a number of other differences between the clarified SAS 70/SSAE and the old SAS 70, which the author believes to be of a more minor nature for CISAs/IT auditors.

[11] AICPA, *Trust Services Principles, Criteria, and Illustrations for Security, Availability, Processing Integrity, Confidentiality, and Privacy*, 2009

Scott M. Baron, CISA, CRISC, CCDP, CCNP, MCSA, MCSE

Scott Baron is director of digital risk and security governance for National Grid, where his team has global responsibility for information systems (IS) risk and compliance efforts. Prior to joining National Grid, Baron worked to pioneer the compliance and business continuity effort at Northwest Airlines, and in 2006, Northwest Airlines became one of the first legacy airlines to achieve and maintain Payment Card Industry (PCI) compliance. Baron also founded the professional services company iNETech, where he worked with customers to develop and implement best practices in networking and information security solutions.

Baron enjoys speaking about IT governance, risk and compliance (GRC) with anyone who will listen and has presented at several conferences. He is a member of ISACA's 2011 ITGRC Conference Development Task Force.

When not working, Baron enjoys music, travel and relaxing with his family. He and his family are self-proclaimed Disney fanatics and have been to Disney World (Florida, USA) more than 10 times since 2006.

Q **What do you see as the biggest risks being addressed by IT auditors and/or security professionals? How can businesses protect themselves?**

A Recent high-profile cases and global politics have triggered a number of new regulations. These new regulations pose a risk to the organization because they come with stricter penalties and are written with less guidance for interpretation. This means that, oftentimes, the requirements outlined in a regulation are interpreted in varying ways depending upon the reader. If the regulators have a different interpretation of the same requirement, it could result in additional work and/or fines. This makes compliance a costly, moving target.

Regulations are typically based on an industry standard and tailored for the specific vertical. Businesses should protect themselves by implementing a standards-based approach to IT, targeting people, processes and technology across the organization, and utilizing a risk-based methodology.

Q **How would you describe the impact of the increasingly strict regulatory environment on IT auditors and security professionals?**

A IT auditors find that they are under an avalanche of assurance requirements. Often, these requirements are similar in nature, but impact different areas within the organization. Security professionals, however, find themselves in an increasingly inflexible environment and can feel like decisions regarding which controls are best for the organization are taken out of their hands.

The new regulatory environment has placed a greater strain on the already taxed workload of IT auditors and security professionals. New skills are required to interpret the regulations, and new processes are required not only to perform a function, but also to prove its effectiveness. Corporations, in turn, struggle to show the value derived from the added cost and increased complexity of compliance.

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 Legacy security professionals are focused on the cause of a security event rather than the effect of the event. This typically results in a risk-averse attitude or a culture of "no." Information security is often perceived as a roadblock rather than a business partner.

New security professionals should focus on business requirements and gain a true understanding of just how each decision will impact the business. True business partners should not try to secure the business, but rather to *enable secure business*. This will go a long way toward ensuring that security has a seat at the table when decisions are made.

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

A Certifications serve to establish a common language and baseline of knowledge within the community. Certifications can inspire a level of confidence in employers and a level of recognition among peers.

While beneficial, some certifications do little to illustrate specific experience, and no certification can demonstrate a solid work ethic. When hiring an assessor position, I look for a candidate with a Certified Information Systems Auditor® (CISA®) certification. When looking to fill a more technical position, I like to see a Certified Information Systems Security Professional (CISSP) certification. These are well-established certifications, and both have experience and continuing education requirements. The new Certified in Risk and Information Systems Control™ (CRISC™) certification shows promise when partnered with CISA.

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

A The modern culture of compliance requires that IT professionals document what and how they are going to do something, manage the asset, and provide assurance that it was done according to plan.

A colleague recently recounted a story about an IT professional who asked, "Do you want me to dig the hole, or do you want me to document how to dig the hole?" Of course, the answer is both, but in addition, the professional has to prove that both were done. As you can imagine, this is an unpopular viewpoint in an already overstressed IT environment.

The solution is cliché. IT organizations need to "work smarter, not harder." They need to build the case that common processes should have the same procedures and controls.

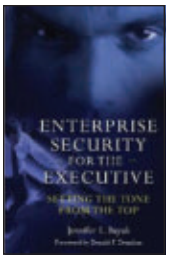
Sharpen your skills and give yourself a major edge in the job market with a cybersecurity degree or a new graduate certificate from University of Maryland University College (UMUC). Our degrees and certificates focus on technical and policy aspects, preparing you for leadership and management roles—and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

- Designated as a National Center of Academic Excellence in Information Assurance Education by the NSA and the DHS
- Advanced virtual security lab enables students to combat simulated cyberattacks
- Financial aid and an interest-free monthly payment plan available

UMUC
University of Maryland University College
Copyright © 2011 University of Maryland University College

Enroll now. | 800-888-UMUC • umuc.edu/cyberedge

Enterprise Security for the Executive: Setting the Tone From the Top



By Jennifer L. Bayuk

Reviewed by C.W. Axelrod, Ph.D., CISM, CISSP, former business information security officer and chief privacy officer for U.S. Trust, Bank of America Private Wealth Management. Axelrod is currently a senior consultant with Delta Risk, which specializes in cybersecurity, risk management and business resiliency. He is a member of the Financial Services Sector Coordinating Council (FSSCC) Research and Development Committee and won ISACA's 2009 Michael P. Cangemi Best Book/Best Article award. He was honored with the Information Security Executive (ISE) Luminary Leadership Award in 2007 and the *ComputerWorld* Premier 100 IT Leaders Award in 2003. Axelrod is the author of the book *Outsourcing Information Security* and coeditor of *Enterprise Information Security and Privacy*, both of which are available in the ISACA Bookstore.

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.

Enterprise Security for the Executive: Setting the Tone From the Top, written by Jennifer Bayuk, appeared in November 2009, just two years after the author's *Stepping Through the InfoSec Program*.

Bayuk's books are typically compact, clearly written, well focused and easy to read, and they are frequently aimed at nontechnical corporate leadership and those information security professionals who see themselves as future managers. Both of these categories of readers will greatly benefit from reading *Enterprise Security for the Executive: Setting the Tone From the Top*.

The author worked as an information security professional in a major investment bank and securities firm for more than a decade. In preparing *Enterprise Security for the Executive*, she drew from her own vast experience and discussions with peers, most of whom were from similar large financial services firms. Therefore, the question arises whether a concentration in financial services such as the experiences depicted in the book can be considered truly representative of other sectors and of small to medium-sized businesses. The answer is "yes."

Lessons from the banking and finance sectors are likely to be learned ahead of most other public and private sectors, and therefore, the experiences of those in this sector remain valuable to those in other sectors. Furthermore, since practically every human economic activity is dependent on the financial services industry, it behooves management in other sectors to understand the security strengths and weaknesses of this critical industry so that they are better equipped to deal with issues they may have with their financial institutions and within their own organizations.

The greatest value of *Enterprise Security for the Executive: Setting the Tone From the Top* is its description of information security practitioners' experiences in dealing with C-level management and how those relationships should be handled. It is unusual to see so many actual experiences included in a single book and presented in such a way that readers can relate each experience to their own situations. Bayuk uses a creative tool in the form of security horror stories (SHSs) to illustrate and drive home the lessons of the text. The SHSs are not meant to impart fear, uncertainty and doubt on the part of the reader or the reader's management, but to "illustrate the fact that, in the absence of systemic security management, disasters do happen."

The book comprises introductory chapters on security threats and vulnerabilities; the security triad of confidentiality, integrity and availability; and secure products and services. Most security professionals should be well versed in these topics, but their managements likely will not match that expertise. On the other hand, the chapters on management structures for the security function and those dealing with legal and regulatory requirements will generally be more familiar to executives than to security engineers. As a result, the book has something for everyone, although it is clearly geared to senior management.

Readers should not skip the case study found in the appendix. While it is hoped that none of the readers are confronted with an environment such as the one depicted in the case, those who, at one time or another, have been tasked with establishing security programs from scratch can readily relate to the story.

As with some of the author's prior works, *Enterprise Security for the Executive* provides valuable advice to the reader. However, the real value of the book is realized when read by senior managers, who are less likely to seek out such a book.

EDITOR'S NOTE

Enterprise Security for the Executive: Setting the Tone From the Top 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. Another resource is the ISACA Business Model for Information Security™ (BMIS™), posted at *www.isaca.org/bmis.*

By Himanshu Dwivedi, Chris Clark and David Thiel

Reviewed by Jeimy J. Cano M., Ph.D., CFC, CFE, CMAS, distinguished professor in the law department of the Universidad de los Andes, Colombia. He has been a practitioner and researcher in information and computer security and in computer forensics for more than 15 years in different industries. Cano is a member of ISACA's 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.

Mobile Application Security

According to an April 2010 Morgan Stanley study on Internet trends,[1] within 10 years there will be a consolidated mobile Internet domain in which applications and interactions between users will become the norm, and information flow will be part of the reason for the services available on that platform.

Similarly, the presence of mobile devices such as smartphones and tablets is an inherent part of the era of mobility and instant information that exists today. In a world dominated by mobility, interaction and loss of privacy, it is necessary to adopt new practices of security and control that enable organizations to meet the challenges of a moving society exposed to continuous data leakage.

In this sense, *Mobile Application Security* introduces the details of current mobile platforms (such as Java Mobile Edition; Symbian OS; webOS; Windows Mobile; and the operating systems of iPhone, Android and BlackBerry) as a way to understand the key aspects of their technical architecture and security issues to establish assurance and control elements that facilitate coexistence in an adequate and reliable mobile reality.

> "New practices of security and control… enable organizations to meet the challenges of a moving society exposed to continuous data leakage."

The book presents a series of suggestions and security tips for developing mobile applications, including the use of protocols such as Transport Layer Security/Secure Sockets Layer (TLS/SSL), input validation, an assurance permission model for the OS, configuration of least privilege and access strategy, proper storage of sensitive information, code signing applications, knowledge of the limitations and advantages of the mobile devices browsers, and safe use of URL.

The authors clearly outline the benefits, risks and security measures for each of the mobile platforms, with examples indicating the actions required for each. Additionally, a review of other mobile services, such as Bluetooth, Wireless Application Protocol (WAP), Short Message Service (SMS) and geolocation, that are inherent parts of the features offered on mobile devices is also provided.

Moreover, analysts offer guidelines based on corporate assurance in the use of these mobile devices, knowing that this is one way to realize data leakage, loss of information and entry of malicious code in the computing infrastructure of enterprises.

Mobile Application Security is intended for information security specialists, information systems (IS) auditors and professionals in IT governance because it includes clear answers about the requirements, risks and control measures required in a mobile information society.

For IS professionals and IT managers faced with securing mobile applications, this book provides a set of best practices that are adaptable to the requirements and business strategies of organizations. These best practices can improve the level of protection and control of information flows on mobile devices while balancing the need for monitoring and control.

ENDNOTE

[1] Morgan Stanley, Internet Trends, 12 April 2010, *www.datam.co.nz/Files/Whitepaper-Internet-Trends-apr2010.pdf*

EDITOR'S NOTE

Mobile Application Security 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. Another resource is the ISACA white paper *Securing Mobile Devices*, posted at *www.isaca.org/research.*

A Cost-effective Approach for Sarbanes-Oxley-regulated Application Systems With Minimal IT Control Assurance

Loic Jegousse, CISA, CISM, CGEIT, CRISC, is an independent technology risk consultant with a track record of removing unnecessary complexity from highly regulated organizations and delivering cost reductions while ensuring that operational and technological risks are managed at an acceptable level. In his past role with MDS Inc., a global life sciences corporation, Jegousse was able to reduce significantly the ongoing costs of regulatory compliance and improve the organization's posture toward internal and external audits.

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 fine-tuning scoping methodology will help provide senior management with greater latitude in deciding whether an application system is deemed in scope for the purpose of an IT control assessment, as mandated by the US Sarbanes-Oxley Act and equivalent regulations/legislation. The proposed approach will assist in reducing reliance on IT automated controls (ITAC) when it makes business sense to do so. This article assumes that baseline data exist regarding the application system and controls deemed in scope.

Many complexities are involved when managing large internal controls programs such as those mandated by legal requirements. Many suggested approaches have been provided to perform comprehensive IT risk assessments so that the scope of the program is focused on areas with the highest risk of financial data integrity. Frequently, compliance assessment teams struggle with the IT-related components of internal control assessments and call their IT auditor/control specialists to evaluate a balanced approach. A typical scoping process within an organization's program is:

1. Senior management defines the scope in terms of materiality, identifies the scope of accounts from the balance sheet and profit and loss (P&L) statement, and then identifies the scope of business locations and business processes that impact these accounts. This step generally does not involve IT auditors/specialists.
2. For a given business process and location, a controls assessment team maps business processes, identifies control activities and then highlights key controls over financial reporting. Control activities are considered either manual or ITAC. Whenever a key control is an application control (such as an automated report or an automated workflow in commercial off-the-shelf software), the supporting application system and underlying IT infrastructure are required to be in scope.
3. The IT auditor/control specialist performs an IT risk assessment to identify the extent of IT work for both the specific application system control and the underlying IT general controls (ITGC), prior to evaluating the control design and operating effectiveness to ascertain control assurance.
4. The IT auditor/control specialist performs the IT assessment (design assessment and operating effectiveness testing) and reports the findings to the senior management team and to the controls assessment team for remediation and evaluation of the control deficiencies in isolation and aggregation.

Here are the issues caused by such a mechanical approach to scoping:

- **Cost**—The number of application systems in scope can be extensive because of the scoping approach, with some application systems supporting only a few key controls over financial reporting. As a result, excessive resources are consumed to assess the IT controls for a wide spectrum of IT assets.
- **Compliance**—The approach does not take into consideration that application systems with only a few application controls may be considered legacy application systems. Such legacy systems are prone to control deficiencies, and there could be little management support to invest in remediation efforts for those if deficiencies were identified. Senior management may be focused on retiring these legacy systems and implementing a brand-new, enterprisewide application instead. As a result, legacy systems deemed in scope are more likely to be the source of deficiencies.

Who wants to spend time testing controls and reporting deficiencies that will remain in the deficiency listing for a long time? Unfortunately, the usual methodologies, i.e., what was described previously, do not necessarily address such a problem. Also, in accordance with the Pareto principle,[1] it could be that 20 percent of the application systems in scope are causing 80 percent of the problems. Therefore, it would be beneficial to come up with a method for identifying easy opportunities for improvement and to build the business case for a compliant and cost-effective control design.

Enjoying this article?

- Read the ISACA publication *IT Control Objectives for Sarbanes-Oxley, 2nd Edition*

www.isaca.org/sox

- Access the Sarbanes-Oxley topic in ISACA's Knowledge Center

www.isaca.org/knowledgecenter

TARGETING THE SOURCE OF THE "NOISE"

Here are the proposed steps to identify the target applications for further analysis:

1. Obtain a current list of application systems deemed in scope and the key application system controls that were identified. Whenever possible, break down application system controls into the following types:
   - Automated control
   - IT-dependent control
   - Application-system-specific access/segregation of duties (SoD) control
2. Evaluate the effectiveness of ITGC for each application system. This can be performed either by reviewing the results of past testing or by performing an abbreviated assessment focused on key areas.
3. Qualify the pervasiveness of the application system relative to the financial statements, i.e., how critical the application system is to the integrity of financial statements as a whole. For instance, an enterprise resource planning (ERP) system would be qualified as "high relative pervasiveness," while an application system supporting only one particular business process for one business location would be qualified as "low relative pervasiveness."
4. Present the data in a table such as the example in **figure 1**. The analysis will then focus on target applications with the following attributes:
   - Low number of application controls, particularly those with few automated controls
   - Low pervasiveness to the financial statements
   - Overall effectiveness of ITGC. It is key to note that controls failure in key areas (e.g., change control, SoD) can impact the overall effectiveness and prevent the team from testing related ITAC using the "test of one" assumption.[2]

In **figure 1**, the target applications are App1 and App2 because they meet the criteria. App3 was not selected based on its "medium" pervasiveness to financial reporting. As further explanation, a number of application controls is deemed "low" based on a comparison to the number of ITGC for the environment. As an example, if there are, on average, 20 ITGC, "low" would probably mean anything between one and 10 application controls.

Following is a look at the target applications identified from the cost and compliance angles:

- **Cost**—For applications systems in which ITGC are deemed ineffective, resources will be required to remediate the

Figure 1—Example Inventory of Application Controls

Attributes	App1 (e.g., billing and revenue for one site in one business unit)	App2 (e.g., billing and revenue for one site in one business unit)	App3 (e.g., billing and revenue for all business units)	...	AppN (e.g., ERP)
Total number of ITAC	1	2	3		40
Pervasiveness to financial reporting	Low	Low	Medium		High
ITGC effectiveness	Ineffective	Ineffective	Ineffective		Effective
Total number of ITGC	20	20	20		20

deficiencies. Also, the testing of the application system controls for those will not meet the requirements for the "test of one" sample, and, therefore, the application system controls will need to be tested like manual controls—increasing dramatically the time needed to assess operating effectiveness.

- **Compliance**—For App1 and App2 in **figure 1**, the application systems are not pervasive to financial reporting; therefore, it is unlikely that the impact of ITGC would be considered significant. However, management will be under pressure to remediate these because, if not acted upon within a reasonable time frame, their ranking could be escalated.

With respect to the target applications with weak IT assurance, management does not seem to have many options available:

- **Option 1**—Postpone the pain, i.e., do not immediately remediate the ITGC deficiencies and then bear the increased cost of performing the testing of automated controls, which may not be prohibitive considering the number of controls. In this scenario, management hopes to postpone funding for remediation.
- **Option 2**—Allocate resources to solve the deficiencies, and aim for effective ITGC. However, management should be made aware that remediation initiatives related to ITGC are complex and that success is not always guaranteed because of the number of "moving parts" involved—for instance, additional staff may be required to satisfy SoD, third-party software may need to be acquired to support monitoring activities, or enhancements may need to be carried out to produce satisfying audit logs.

"OPTION 3"—CONTROL REEVALUATION CONSIDERATION

An alternative option should be contemplated, whereby the application system controls are *substituted* to a strong manual control. This alternative strategy is the core of this article and relies on the team's ability to think from the perspective of the business and articulate the decisions in terms of costs/benefits. The selling point is that in instances such as described previously, i.e., weak IT controls with limited use of automated controls, it is often cheaper and more effective to implement key manual controls rather than rely on automation. This will sound counterintuitive to many readers, and of course, this method is not recommended in areas in which IT systems are relied on pervasively. Here are the proposed steps to reach a decision regarding the control design and the trade-offs between automation and manual operation:

1. For a given target application, review existing high-level documentation of the environment that relies on the application system. This includes reviewing the financials, processes, list of control activities and systems involved. Identify the names of key business stakeholders (such as general manager, controller, process owners and IT manager).
2. Determine the materiality threshold for the environment supported by the target application. As a rule of thumb, use a prorated calculation of the overall materiality threshold. For example, if the overall materiality is US $10 million for a significant deficiency and the environment that the target application supports represents 10 percent of the business, the threshold to consider would be a US $1 million annual misstatement.
3. Schedule a workshop with representation from both the business and the controls assessment team. The business representatives should have sufficient authority to make decisions in line with their accountabilities. The control assessment team should represent skills for the entire controls area—both business process and IT controls. An important point is to articulate in advance the goal of the workshop in order to maximize attendance and chances of success. At the end of the day, a decision is needed regarding the design of key controls so that costs and compliance profiles will be improved.
4. Start the workshop by restating the objective, describing the problem in terms of costs and compliance, and outlining the three options available along with the costs and benefits of each.
5. Walk through the process whereby the target application is involved (one application at a time) for the key controls. Then, hypothetically assume that, for whatever reason, the application system cannot be relied on, i.e., that the data lack integrity—regardless of the cause (processing error, unauthorized access to database, etc.). In most cases, it may turn out that, for the hypothetical failure of the target application to result in a significant deficiency, it would require a combination of operational breakdowns that would go unnoticed for a prolonged period of time.

The discussion may reveal new mitigating controls that

were not identified before. Also, the participants may realize that it could be quite easy for the business to implement a reasonableness check that would validate, on a regular basis, that the target application output is within range of acceptable value, i.e., within the agreed-on materiality threshold. Whatever existed as an informal control could then be turned into a strong key control—with the corresponding audit ability requirements. The business may initially be reluctant to accept the extra burden of operating a new manual key control, but will certainly recognize that the proposed "third option" is cheaper and/or more compliant than options 1 and 2 (noted previously).

CONCLUSION

A cost- and risk-effective approach is derived from a holistic view of the objective and from evaluating options for conformance based on the business control environment and culture. If workshops were completed successfully for App1 and App2 of **figure 1** and the business agreed to implement a total of three new manual key controls to replace the three application controls, ITGC testing would no longer be required, saving approximately the cost of testing 40 controls. Remediation would be still encouraged, but with decreased pressure from the controls assessment team. (Note: from a strict financial reporting standpoint only—there may be other rationale to drive remediation efforts.) Implementing the new manual controls is likely to cost less than remediation of ITGC deficiencies. As a result, senior management can now allocate resources to where they are the most needed in the organization—to the benefit of the organization's stakeholders.

ENDNOTES

[1] The Pareto Principle (also known as the 80/20 rule) states that for many events, roughly 80 percent of the effects come from 20 percent of the causes. The principle is named after Italian economist Vilfredo Pareto, who observed in 1906 that 80 percent of land in Italy was owned by 20 percent of the population. Koch, Richard; *The 80/20 Principle: The Secret of Achieving More With Less*, Random House, USA, 1998

[2] Rajamani, Baskaran; "Certifying Automated Information Technology Controls: Common Challenges and Suggested Solutions," Deloitte, *www.deloitte.com/view/en_CA/ca/services/ceocfocertification/article/c1fcfa9d452fb110VgnVCM100000ba42f00aRCRD.htm*

IT Scenario Analysis in Enterprise Risk Management

Urs Fischer, CISA, CRISC, CPA Swiss, is an independent IT governance, risk and compliance consultant. From 2003 to 2010, he was vice president and head of IT governance and risk management for the Swiss Life Group. Previously, he was head of IT audit for the SwissLife Audit Department based in Zurich, Switzerland. Since 1989, Fischer has worked in the IT governance, audit and security areas and has gained extensive IT governance, risk management and information systems compliance experience. Involved in the development of COBIT® 4.0 and 4.1, he is also helping with the development of COBIT 5. A member of ISACA's Guidance and Practice Committee, in June 2010, he received the John Lainhart IV Award from ISACA.

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.

Scenarios are a powerful tool in a risk manager's armory—they help professionals ask the right questions and prepare for the unexpected. Scenario analysis has become a 'new' and best practice in enterprise risk management (ERM) (see **figure 1**). Scenario analysis is also a centrepiece of ISACA's Risk IT framework.[1, 2]

Risk scenario analysis is a technique to make IT risk more concrete and tangible and to allow for proper risk analysis and assessment.[3] It is a core approach to bring realism, insight, organisational engagement, improved analysis and structure to the complex matter of IT risk.

SCENARIO ANALYSIS FLOW

One of the challenges for IT risk management is to identify the relevant risks amongst all that can go wrong. A technique to overcome this challenge is the development and use of risk scenarios. Once these scenarios are developed, they are used during the risk analysis, in which the frequency of the scenarios occurring and the business impacts are estimated.

Figure 2 shows that IT risk scenarios can be derived two different ways:

- A **top-down approach**, in which one starts from the overall business objectives and performs an analysis of the most relevant and probable IT risk scenarios that are impacting the business objectives
- A **bottom-up approach**, in which a list of generic scenarios is used to define a set of more concrete and customised scenarios

The approaches are complementary and should be used simultaneously. Indeed, risk scenarios must be relevant and linked to real business risks. On the other hand, using a set of example generic risk scenarios helps ensure that no risks are overlooked and provides a more comprehensive and complete view of IT risk.

The following is a practical approach that has been proven helpful in developing a set of relevant and important risk scenarios:

1. Use a list of example generic risk scenarios[4] to define an initial set of concrete risk scenarios for the organisation.
2. Perform a validation against the business objectives of the organisation.
3. Refine the selected scenarios based on the validation; categorise them to a level in line with the criticality[5] of the organisation.
4. Reduce the number of scenarios to a manageable set.[6]
5. Keep all risks in a list so they can be re-evaluated in the next iteration and included for detailed analysis if they have become relevant at that time.
6. Include 'unspecified event' in the scenarios to address incidents that are not covered by the specified scenarios.

Once the set of risk scenarios is defined, it can be used for risk analysis. In risk analysis, frequency and impact of the scenario are assessed. Important components of this assessment are the risk factors, which are described in the next section.

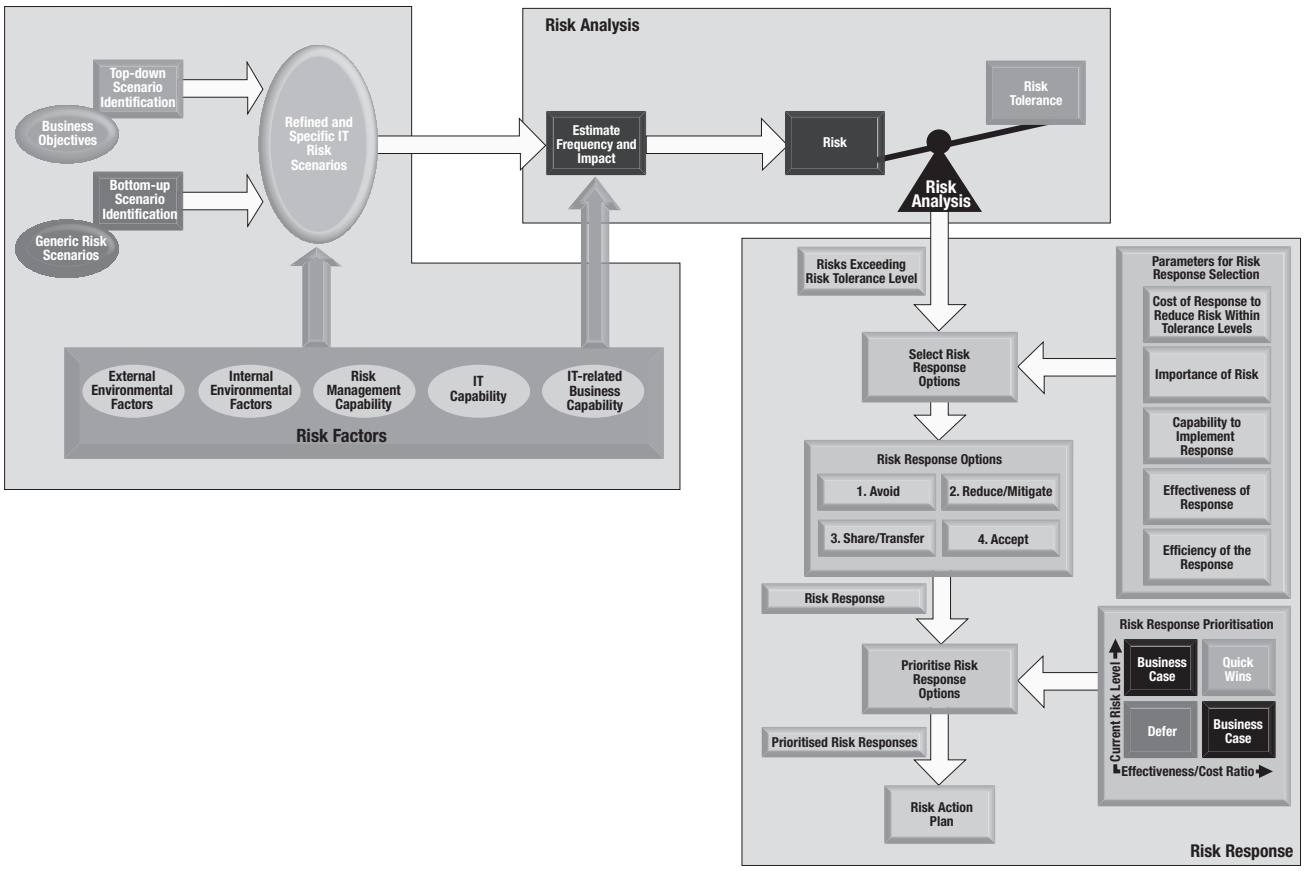
This is not rocket science, so why do organisations fail to use risk scenarios more often and routinely? Keep in mind that scenarios are in fact harder to develop than they seem. A good scenario takes time to build and requires good input from a number of areas of the enterprise; therefore, a whole set takes a large investment of time and energy.

RISK FACTORS

Risk factors are factors that influence the frequency and/or business impact of risk scenarios. They can be of different natures and can be classified in two major categories:

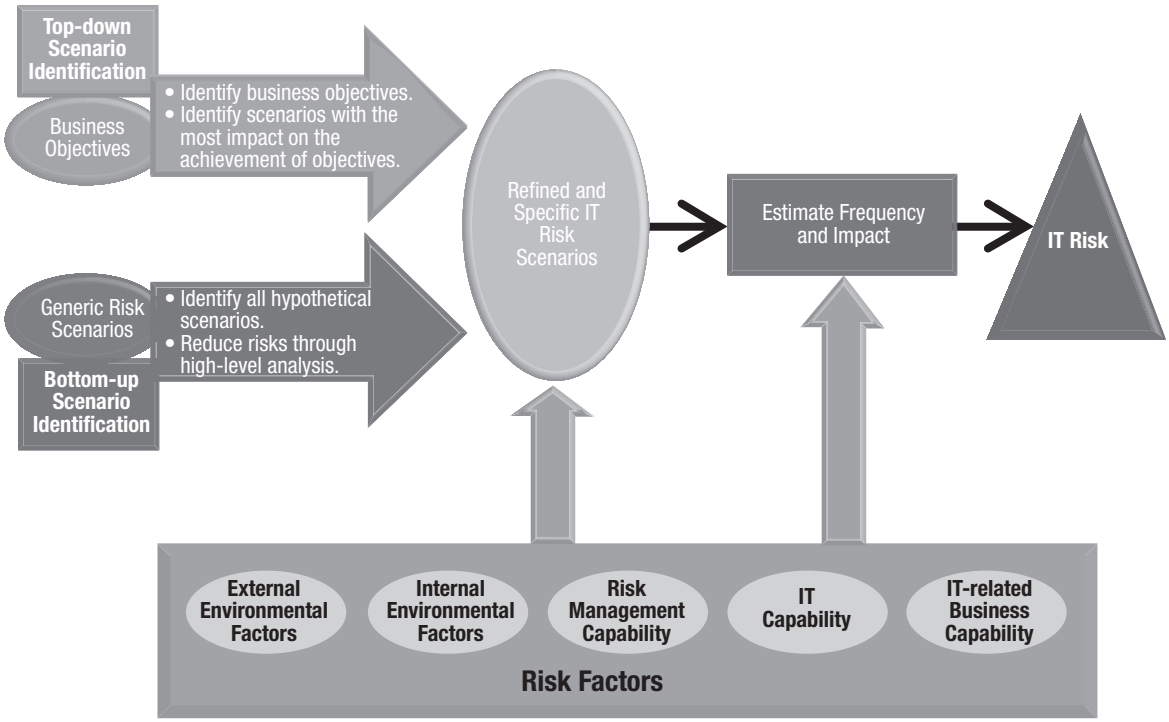
- Environmental factors, which can be divided into internal and external factors—the difference being the degree of control an enterprise has over them:
  - Internal environmental factors are, to a large extent, under the control of the enterprise.
  - External environmental factors are, to a large extent, outside the control of the enterprise.
- Capabilities, i.e., how good the enterprise is in a number of IT-related activities. They can be distinguished in line with ISACA's three major frameworks:

Figure 1—Risk Analysis and Risk Response Overview



Source: ISACA, *The Risk IT Practitioner Guide*, USA, 2009

Figure 2—IT Risk Scenario Development



Source: ISACA, *The Risk IT Framework*, USA, 2009

– IT risk management capabilities—To what extent the enterprise is mature in performing the risk management processes defined in Risk IT
– IT capabilities—How good the IT processes are, as defined in COBIT
– IT-related business capabilities (or value management)—Expressed through the Val IT processes

The importance of risk factors lies in the influence they have on IT risk. They are heavy influencers of the frequency and impact of IT scenarios and should be taken into account during every risk analysis, when frequency and impact are assessed. **Figure 3** depicts risk factors.[7]

COMPONENTS OF RISK SCENARIOS

An IT risk scenario is a description of an IT-related event that can lead to a business impact, when and if it should occur. For risk scenarios to be complete and usable for risk analysis purposes, they should contain certain components, as shown in **figure 4**.

SCENARIO DEVELOPMENT

The use of scenarios is key to risk management, and the technique is applicable to any enterprise. Each enterprise needs to build a set of scenarios (containing the components described previously) as a starting point to conduct its risk analysis. Building a scenario means that each possible value of every component is combined. Each combination should then be assessed for relevance and realism and, if found to be relevant, entered into the risk register. In practice, this is, of course, not possible because it would result in far too large a number of scenarios. The number of scenarios to be developed and analysed should be kept to a much smaller number to remain manageable, since every possible combination cannot be retained.[8]

Enjoying this article?

- Read the ISACA publication *Global Status Report on the Status of Governance of Enterprise IT (GEIT)—2011*

www.isaca.org/research

- Join this author at the 2011 Asia-Pacific CACS conference in Dubai, UAE, where he will deliver a workshop on IT risk management and using ISACA's Risk IT framework, and at the 2011 EuroCACS Conference in Manchester, England, UK

www.isaca.org/asiacacs
www.isaca.org/eurocacs2011

- Access the Risk Management topic in ISACA's Knowledge Center

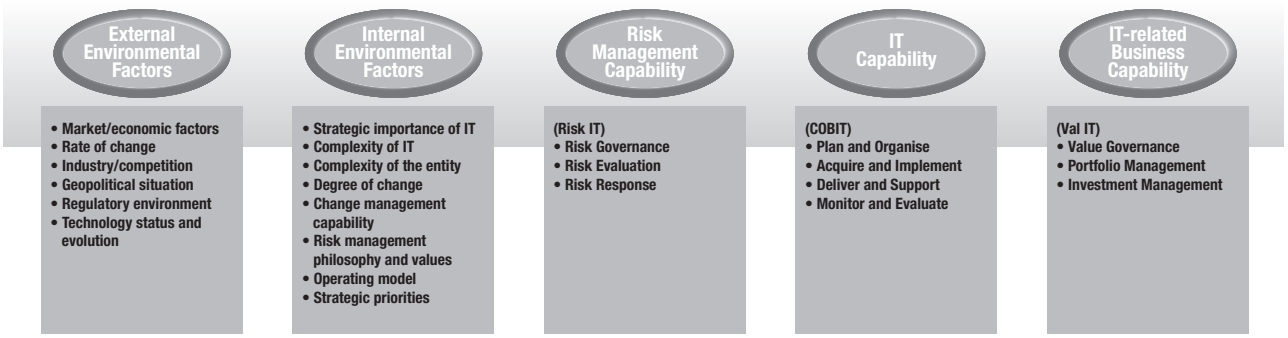
www.isaca.org/knowledgecenter

CONCLUSION

Scenarios have three benefits that make them very powerful for understanding risks and opportunities.[9]

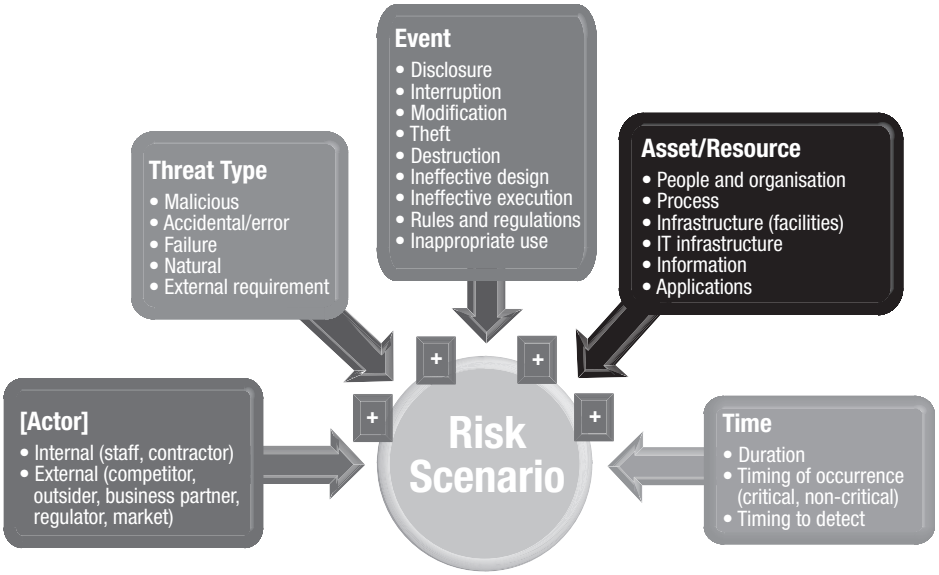
First, *scenarios expand one's thinking*. People will think more broadly if they develop a range of possible outcomes. By demonstrating how—and why—things could quickly become better or worse, they increase their readiness for the range of possibilities the future may hold.

Figure 3—Risk Factors in Detail



Source: ISACA, *The Risk IT Practitioner Guide*, USA, 2009

Figure 4—IT Risk Scenario Components



Source: ISACA, *The Risk IT Framework*, USA, 2009

Second, *scenarios uncover inevitable or near-inevitable futures*. In developing scenarios, people will search for predetermined outcomes—particularly unexpected outcomes, which are often the most powerful source of new insight uncovered in the scenario-development process.

And, finally, *scenarios protect against 'groupthink'*. Often, the hierarchy of an organisation inhibits the free flow of debate. Employees will wait (especially in meetings) for the most senior executive to state an opinion before venturing their own, which then often magically mirrors that of the senior person. Scenarios allow the organisation to break out of this trap by providing a political 'safe haven' for contrarian thinking.

Scenarios will not provide all the answers, but they help executives ask better questions and prepare for the unexpected. That makes them a very valuable tool indeed.

ENDNOTES

[1] ISACA, *The Risk IT Framework*, USA, 2009

[2] ISACA, *The Risk IT Practitioner Guide*, USA, 2009

[3] Risk analysis is the actual estimation of frequency and magnitude/impact of a risk scenario. Risk assessment is a slightly broader term and includes the preliminary and ancillary activities around risk analysis, i.e., identification of detailed risk scenarios and definition of responses.

[4] *The Risk IT Practitioner Guide* provides a list of generic IT risk scenarios. This list can be used as a basis to build the enterprise's own set of relevant risk scenarios.

[5] Critical entities deserve to have risk scenarios defined at a detailed level; non-critical entities can do with quite generic scenarios that are not elaborated in too much detail. Note that the entity can be an organisational unit, but can also be something cross-organisational, e.g., a grouping of similar business processes and activities.

[6] 'Manageable' does not signify a fixed number, but should be in line with the overall importance (size) and criticality of the unit. There is no general rule, but if scenarios are reasonably and realistically scoped, the enterprise should expect to develop at least a few dozen scenarios.

[7] Risk factors are discussed in detail in *The Risk IT Practitioner Guide.*

[8] Some guidance and considerations for the development and maintenance of manageable numbers of relevant scenarios can be found in *The Risk IT Practitioner Guide*.

[9] Based on Roxburgh, Charles; 'The Use and Abuse of Scenarios', *McKinsey Quarterly*, November 2009

Key Considerations When Evaluating ISRM Programs and Capabilities

John P. Pironti, CISA, CISM, CGEIT, CRISC, CISSP, ISSAP, ISSMP, is president of IP Architects LLC. He has designed and implemented enterprisewide electronic business solutions, information security and risk management strategy and programs, enterprise resiliency capabilities, and threat and vulnerability management solutions for key global customers in a range of industries, including financial services, insurance, energy, government, hospitality, aerospace, health care, pharmaceuticals, media and entertainment, and IT. Pironti frequently provides briefings and acts as a trusted advisor to senior leaders of numerous organizations on information security and risk management and compliance topics and is also a member of a number of technical advisory boards for technology and services firms.

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.

Traditionally, information security and risk management (ISRM) has often been perceived as a barrier to success and a disabling force within organizations and business leadership—instead of as a benefit and an enabling capability. This perception is typically a result of the traditional perception of technology: providing security first and using fear, uncertainty and doubt to invoke the need for security within organizations. However, a mature ISRM program and capability is an enabler to the organization and, in many cases, considered a strategic advantage in business activities.

ISRM programs and capabilities have become vital elements within most organizations as they realize the value of their data and information infrastructures. These capabilities have quickly matured beyond foundational requirements and now need to be managed and matured to ensure alignment with business expectations and activities. The accurate and continual evaluation of these programs and capabilities by examiners is critical to their success and to understanding their benefits and challenges to the organizations and constituencies they serve.

EVALUATION METHODS

There are numerous methods and practices that can be used to evaluate the ISRM program and capabilities of an organization, including surveys, interviews, artifact and evidence reviews, benchmarking, capability maturity modeling, and capability alignment with industry-recognized and industry-leading functional inventories. Independently, each of these provides value to the evaluator and the business, but by themselves, they do not provide a comprehensive perspective to all interested parties. It is often optimal to combine these capabilities and use them together to ensure that an accurate and complete view.

Using a customized version of the Capability Maturity Model (CMM) (**figure 1**) to evaluate ISRM programs and capabilities is often the most effective, comprehensive and widely recognized method. While originally developed for the software industry, CMM can be easily adapted for ISRM program and capability analysis. By adding an incrementing scale within the individual layers of the traditional CMM model, an evaluator can provide details about the maturity of an organization and capabilities that are often requested by organizational leadership and stakeholders. The incrementing scale should represent three distinct segments: .1 through .3 represent capabilities that are in their initial state of maturity, .4 through .6 represent stabilized maturity, and .7 through .9 represent progression toward the next level of maturity.

Figure 1—ISRM Capability Maturity Model

Maturity Level	General Description
5	Optimal, optimizing, business-aligned
4	Managed, controlled, predictable
3	Proactive, defined, implemented
2	Repeatable, reactive, best effort
1	Initial, undefined, *ad hoc*
0	Intent, not identified

Increment Range	Increment Description
.7-.9	Progressing
.4-.6	Stablized
.1-.3	Initial

A leading way to evaluate ISRM programs and capabilities is to utilize functional inventories as a baseline for the evaluation of functions and a review of the governance models that are being used. In the case of ISRM, two functional inventories are applicable: the information security program (**figure 2**) and the information risk management program (**figure 3**). These inventories include the services and capabilities that should be evident within an organization if it has implemented comprehensive programs and capabilities.

Figure 2—Information Security Program Functional Inventory

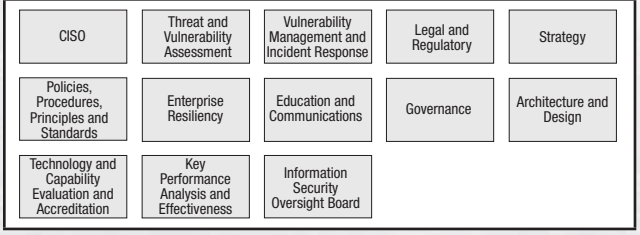
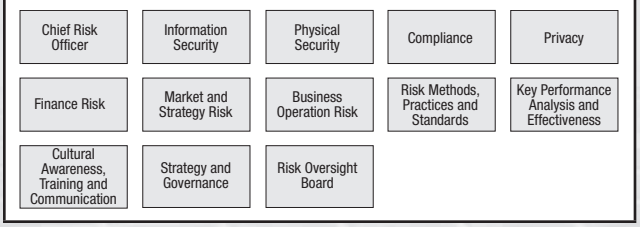


Figure 3—Information Risk Management Program Functional Inventory



Once the functional inventories that are going to be used are identified, it is important to evaluate the strategy that the organization has developed for the ISRM program and capabilities to ensure that it is aligned with business expectations and requirements.

EVALUATING ISRM STRATEGY

It is important to assess whether an organization has developed and implemented a formal strategy for the ISRM program and associated capabilities, and that it has been documented and approved within the organization. A comprehensive strategy will include, at minimum, the following key elements:

- Comprehension and acknowledgment of current business conditions
- Governance models that will be utilized
- Alignment with the organizational risk profile and appetite
- Budget considerations and sourcing plans
- Metrics and measures
- Communication and awareness plans

Strategy is an important component to evaluate. It must be carefully considered and executed to align with business requirements and expectations.

BUSINESS ALIGNMENT AND ACCEPTANCE

The alignment of ISRM capabilities with business requirements and activities is vital to the ISRM program's success. Polling and interviewing business stakeholders and leaders about their perceptions and interactions with the ISRM organization and its functions are the leading methods for assessing business alignment. The business and other interested parties, such as external stakeholders and regulatory oversight groups (if applicable), should not only be aware of the capabilities that are provided, but also be able to derive value from the knowledge and services that are furnished. A key indicator of the lack of business alignment is the business or any interested party being unhappy with or unaware of the capabilities or services that are provided or available.

An additional consideration when evaluating business alignment is the ability of the ISRM program or capabilities to assist in the enhancement of business activities and financial position. ISRM can be used as a valuable asset to increase the confidence of current and prospective customers and partners when they are deciding to begin or enhance a business relationship with an organization. A key indicator of the existence of this capability can be found in the sales and marketing approaches of the organization. Including ISRM concepts and capabilities in messaging or communication activities shows confidence in these capabilities and acknowledges their strategic value potential.

A key indicator of business acceptance is the time in the development cycle of products and services at which ISRM programs and capabilities are engaged. Often, organizations that utilize ISRM capabilities early in their development activities find that they are able to reduce costs (often by as much as 30 percent) and increase efficiency in those capabilities. This is because the organizations integrate ISRM concepts and requirements in the design phase, not toward the end of development activities when the need to add these capabilities results in costly reengineering and adjustments.

Another key indicator of ISRM business acceptance is the number of policy exception requests that are applied for by the business and then granted by the ISRM organization. It is typical to see an increased or higher-than-normal number of exception requests (compared to existing policies) when new policies are introduced. Exceptions that are requested based on the need for more time to comply with the policies are not as critical as those that are requested as an attempt

Enjoying this article?

- Make sure to attend one of the three ISRM conferences scheduled for 2011

  www.isaca.org/isrm

- See the ISACA Business Model for Information Security (BMIS)

  www.isaca.org/bmis

by the business to evade or avoid complying with policies. More important than the number of requests is the number of approvals that are granted for the requests. A large number of requests and approvals is a key indicator that the policies are not aligned with the business needs or capabilities.

GOVERNANCE

To function at optimal efficiency and capability, ISRM programs and capabilities require a governance plan and structure to be in place and functioning. The governance model should include the functional inventory that is utilized and an operating plan for each function. This plan should include staff and resource requirements, budget tracking, maturity and stabilization plans, a mapping to strategic business goals and requirements, and evidence of business alignment. The governance model should also clearly define the minimal and optimal operating requirements for each function and show evidence of tracking activities that demonstrate that the leadership of both the ISRM program and the business has accurate and meaningful insights into the health and performance of the program and of the services and capabilities that are provided by the program.

The reporting structure of the ISRM program is key to its ability to be effective and successful within an organization. Many ISRM programs were created as part of technology organizations and are reported on to the chief information officer (CIO). This can be an effective structure for initial capabilities, but it is often not ideal or appropriate for mature organizations. The goal of ISRM should be to protect information and the information infrastructure, which includes technology, but it should not focus on this alone. When reviewing ISRM capabilities, areas should be noted in which a conflict of interest may arise due to ISRM leadership's interaction with members of technology leadership who may not understand or support the full scope of the capabilities and requirements.

Once the governance structure has been evaluated, the next key area of evaluation should be the threat, vulnerability and risk assessment methods and practices that are used by the ISRM program to appropriately identify, evaluate and report on the key areas of risk and concern on which the business should focus at any given time.

THREAT, VULNERABILITY AND RISK ASSESSMENT METHODS

The methods and practices that are used as part of ISRM programs and capabilities to evaluate threats, vulnerabilities and risks should be consistent, repeatable and easily understood by their target audiences. These methods and practices should include the following components:

- Business process mapping
- Asset inventory and classification
- Threat and vulnerability analysis methodology
- Risk assessment methodology
- Intelligence gathering, processing and reporting capabilities

A clear distinction must exist between threat and vulnerability analysis and risk management activities within the organization. Information security professionals often mischaracterize situations that are threats and vulnerabilities as risks because the professionals recognize the technical impact without appropriately understanding or incorporating the business impact into their assertions. In most cases, information security programs and the professionals who work in them do not have the full insights of the business leadership in regard to business strategy, importance rankings of business processes and capabilities, and business intelligence to properly identify and rank risks. However, the information they provide about threats, including probability and business impact insights, is essential to the accuracy and value of risk assessments and rankings.

When evaluating ISRM capabilities, a key area of focus should be the process utilized to identify and represent risk to the organization and key stakeholders. Risk assessment, ranking and reporting capabilities should utilize and follow a structured, consistent and repeatable approach. The ISRM capabilities of an organization can provide valuable insights into the enterprise risk management (ERM) capabilities

of the organization, and are often better suited to perform information risk assessments and rankings for the enterprise. ERM often does not have the maturity or knowledge to properly incorporate information risk into their assessment, ranking and reporting. Consequently, the ISRM program and capabilities should work closely with the ERM organization and associated stakeholders to understand their needs and to assist them with their activities.

MODES OF OPERATION

ISRM programs and capabilities are unique within organizations because they have proactive and reactive responsibilities. It is important to assess the ability to effectively operate in both modes. Mature programs are often more focused on proactive capabilities such as threat and vulnerability analysis, vulnerability management, training and awareness, intelligence activities, and control maturity and enhancement. Reactive programs tend to be focused on compliance activities and on responding to incidents and threats as they are realized. If an organization is focused on reactive capabilities, it is often a key indicator of immaturity and a lack of organizational focus on ISRM programs and capabilities.

When evaluating ISRM programs and capabilities, it is important to identify their charter and what they are expected to protect or what problem they are trying to solve. Typically, there are two modes of operation that are utilized. The first is a primarily reactive and technologically focused approach. This model is often found in organizations that do not have mature capabilities and/or do not derive business value from ISRM. In this case, the organization typically does not adequately fund its ISRM program, relies on these capabilities only when it is negatively impacted by an information security incident, and utilizes them as response capabilities.

The second mode of operation, a data- and business-process-focused approach, is typically indicative of a more mature organization. In this mode, the organization perceives ISRM as providing business value, will leverage these capabilities in its revenue-generating business activities, and will embrace the guidance and functions that are provided as a benefit to the organization's success, rather than as a disabling roadblock. In this mode, technology is still incorporated in the activities of ISRM capabilities, but they are more focused on business processes and data in these activities. In most cases, technology becomes a supporting element and is used to enable controls instead of being the primary focus of the ISRM activities.

Either mode of operation can assist the organization in meeting its compliance goals (internal and external, if applicable). The extent to which this should be evaluated and scrutinized will be based on the organization's approach to compliance.

APPROACH TO COMPLIANCE

Compliance has quickly become an integrated part of any ISRM program or capability within an organization. There are numerous external regulatory, legal and industry standards and internal policies with which organizations need to be compliant to meet their compliance goals. One consideration that must be made is the organization's approach to compliance. Ideally, compliance should be considered a starting point and not an end point of ISRM capabilities. Unfortunately, many organizations have adopted an approach called "security by compliance," which is not only a sign of immaturity, it may also make them vulnerable to a significant number of business-impacting threats and may expose them to a wide range of risks for which they may not properly account.

Security by compliance is often an indicator of an organization's distrust or frustration with its current ISRM capabilities. Compliance requirements have provided organizations a measure by which they believe they can gauge their needs for ISRM capabilities. Again, compliance should be considered a starting point and not an end point for ISRM programs, capabilities and requirements.

A key attribute of mature and effective ISRM programs and capabilities is their ability to meet internal and external compliance requirements and goals with minimal effort as a result of their business-as-usual activities. Compliance is not treated as a separate initiative or program, but instead as an integrated component of the organization's business activities. In many cases, proof of compliance will become a data-packaging and reporting activity, with a small amount of effort required to meet specific requirements or to develop reports that may not be part of the normal business operations of an organization.

A compliance strategy should also be part of any compliance-related activities. Complete compliance may not be desirable or achievable given an organization's current business conditions or activities. In this case, it is important that a strategy and road map exist that highlight and focus on the most critical compliance requirements first, and then address other requirements based on business impact and the level of effort required to achieve the requirements over a reasonable period of time.

Along with a strategy for compliance, training and awareness activities also need to be evaluated and considered for their effectiveness. Training and awareness are essential to the concept of cultural change and critical to the success of achieving the goals of business-as-usual activities.

TRAINING AND AWARENESS

Training and awareness activities for ISRM are essential to the success of any capability or program. Training and awareness should not be limited to annual training activities or one platform (electronic, lecture, broadcasts, etc.). When evaluating training and awareness activities, it is important to determine whether the organization has identified the learning styles of its stakeholders and constituency and whether it develops aligned materials.

Training and awareness activities should allow for interactive and bilateral opportunities for learning and communication. It is important that the intended audiences have the ability to ask questions, express concerns and/or suggest ideas. Electronic means such as an internal web site with frequently asked questions (FAQs), blog posts, social media capabilities, and direct contact options with ISRM leadership and staff demonstrate an organization's commitment to working with its constituency instead of being authoritative and omniscient in its approach.

One approach to evaluate the effectiveness of an ISRM program's training and awareness capabilities is to choose employees at random and poll them about their knowledge and impression of the program. The individuals who are chosen should represent a cross-section of the organization, including individual contributors, managers and organizational leaders, and should be asked the same questions. By correlating the data obtained from polling each of these groups, a clear understanding of the awareness of the ISRM program and its capabilities can be derived by its intended constituency and documented.

Correlating data and reporting the results to business leaders and stakeholders are activities that are often associated with metrics and measures. Organizational leaders often base their opinion of the business value provided and of the effectiveness of ISRM programs and capabilities on the metrics and measures that are provided to them.

METRICS AND MEASURES

Metrics and measures help professionals evaluate the capabilities of their business units and functions. ISRM programs and capabilities have become more engrained within organizations as independent business functions and business units instead of as elements within technology programs. These programs and capabilities need to demonstrate business value to their constituencies, including the organizations that they serve. The metrics and measures associated with ISRM capabilities should demonstrate a focus on the value provided by the individual functions and services that they offer, and on the maturity and efficiency of their functional capabilities.

One of the key performance indicators of the metrics and measures capabilities of an organization is the methods and practices that are utilized for development and operation. A consistent and repeatable methodology should be used for the creation of metrics and measures and for the data gathering, analysis, reporting and threshold assignment elements. If metrics and measures are changed frequently (less than one year would be atypical), the data that are collected and reported using them may not be accurate or representative of what is being measured.

Each key metric or measure (those that are collections of multiple metrics and measures or are considered critical to the success of the organization) should also include thresholds with associated actions or activities. Metrics and measures without thresholds do not provide insights into the positive or negative meaning of the values that they produce. Thresholds can be as simple as a notification or as complex as a trigger for a series of actions and activities that will be executed once met. The intended audiences that will be required to take an action or that will be impacted by an action once the threshold is achieved should be able to easily understand the business need or justification for the action and appreciate the value provided to the organization.

Reporting may be the most valuable and important area to review closely when evaluating metrics capabilities. Reporting is the culmination of all of the metric and measurement activities, and is ultimately how the information will be presented to the organization. A key consideration of reporting is audience identification and alignment. In most cases, ISRM programs provide data to a variety of interested parties including senior leadership, business process owners, and technical and operations staff. The reporting of the metrics and measures should be tailored to each of these audiences in the presentation and format and by which data are included. One way to evaluate the reporting capabilities is to interview stakeholders who are recipients of the data for each identified audience type, gauge the value they believe

they receive from the reports and identify how they use the reports in their business activities. If the reports are used for business activities or are reviewed only because the recipients perceive that they need to do so to meet an expectation of leadership, these reports need to be revisited to ensure that they provide consistent business value to the recipients.

OPERATIONAL VS. CONSULTATIVE APPROACH

ISRM programs can include operational components as part of their core capabilities, or they can operate in an advisory and consulting capacity. If operational components are included, there should be a clear definition of expectations of the operational responsibilities and how they differ from other operational capabilities within the organization. There should also be documented processes and procedures for sharing information about operational effectiveness, requirements, intelligence and incident-response activities.

If the approach is purely advisory and consultative, the services that are provided to the organization should be clearly documented, as should the level of effort and interaction with the business that will be required for the services to be successful. Providing guidance and advice without operational responsibilities allows an ISRM program to be viewed positively from within organizations since it is limited in its abilities to prevent organizations from implementing operational capabilities not in agreement with the ISRM program.

INDUSTRY STANDARD ALIGNMENT

There are numerous ways in which an ISRM program can demonstrate its capabilities to interested parties and third-party examiners, but typically the most effective include a demonstration of the alignment of capabilities to industry regulations and/or standards. Industry standards tend to be accepted as industry-leading practices or, at a minimum, as a demonstration of minimal competency and capability. When evaluating ISRM capabilities, it is important to identify what, if any, standards with which an organization is attempting to align, and for what reason. If organizations are aligning purely for the purpose of meeting compliance guidelines, they may not understand or be receiving the benefits that are intended by the standards. If they are treating the standards as guidelines by which they are modeling their services and capabilities, this may be a sign of immaturity since they are reliant on the point of view of outsiders rather than the development of their own best practices.

Industry standards alignment does have many benefits for an ISRM program or capability. An indication of effective alignment will be a mapping of an organization's existing capabilities to those prescribed by the standards that the organization finds useful or beneficial to the business. This method demonstrates that the organization has a thorough understanding of the standards to which it is aligning, as well as an appreciation for the need to develop its own capabilities independently. Some of the key industry standards (or good practices) with which ISRM organizations and capabilities may elect to demonstrate alignment include:

- ISO 27001-27008 and 31000
- US National Institute for Science and Technology (NIST) 800 series of standards
- Payment Card Industry Data Security Standard (PCI DSS)
- COBIT

CONCLUSION

The business value and impact of ISRM programs and capabilities are rapidly being recognized within organizations. ISRM programs are no longer subservient to other capabilities and need to be evaluated and assessed on a regular basis to ensure that they continue to align with the needs and requirements of the organizations they serve. Effective evaluation will allow an organization and its leadership to understand how their ISRM capabilities align with their expectations and industry-leading practices, and where investment needs to be made to meet their needs and requirements.

REFERENCES AND FURTHER READING

Nolan, Richard L.; "Stages of Growth Model for IT Organizations," *Harvard Business Review*, 1973

Humphrey, Watts; *Managing the Software Process*, Addison Wesley, USA, 1989

Pironti, John; "Developing an Information Security and Risk Management Strategy," *ISACA Journal*, vol. 2, 2010

Pironti, John; "Key Elements of an Information Risk Management Program," *Information Systems Control Journal*, vol. 2, 2008

Pironti, John; "Key Elements of an Information Security Program," *Information Systems Control Journal*, vol. 1, 2005

The Struggle for Privacy and the Survival of the Secured in the IT Ecosystem

Building a Holistic Privacy Archetype

Sudhakar Sathiyamurthy, CISA, CIPP, ITIL, MCSE, works for the Enterprise Risk Services group of a Big Four advisory division. Sathiyamurthy's areas of expertise include strategic consulting on IT governance, IT service management, IT process transformation, IT consolidation, IT risk management, and IT security and privacy services. Sathiyamurthy can be contacted at *sudhakarsathiyam@gmail.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.

Businesses are transforming rapidly, and the technologies that evolved over the cumulative innovations of the past half-century have now begun to bring remarkable changes in the way information is managed. Although these technological innovations claim to have offered the opportunity to foster a colossal capability to capture, analyze and disseminate information, they have exemplified an associated increase in the threats to the privacy of information. Perhaps to a greater extent than ever before, current-day businesses face substantial challenges in managing the privacy of information due to the demands posed by globalization, emerging technologies and the changing regulatory landscape.

In light of the previously mentioned facts, it becomes all the more imperative for a business to find a firm foothold in ensuring the best privacy management track record in the market. This article proposes a holistic privacy archetype that provides a pragmatic approach for the business to efficiently manage and stay abreast of growing regulatory and fiduciary requirements.

THE REGULATORY LANDSCAPE AROUND DATA PRIVACY

Privacy is essential to accomplish consumer protection. The focus on the privacy of information is gaining momentum among nations due to the burgeoning use of personal and sensitive information, the cross-functional dependency of information by businesses, and the rising number of data breaches from lack of adequate controls. According to a special report article in *Forbes*,[1] 11.2 million people were victims of identity theft or a related fraud in 2009—at an estimated cost of US $54 billion. Welcome to the world of information—where every bit of data has an associated financial quotient, which is what motivates intruders.

The regulatory landscape across the world prescribes and proscribes measures to protect the privacy of information to counteract emerging threats. **Figure 1** provides a list of regulations across regions of the world (it is not necessarily all-inconclusive). However, the rules are not always alike and have been enacted in relation to a region's cultural, sociological and innate privacy threat factors. Although these regulations have played a key role in modernizing the IT compliance system, they make compliance complex because of globalization. Globalization brings new challenges for information that is exposed to multiple regulatory requirements while crossing borders.

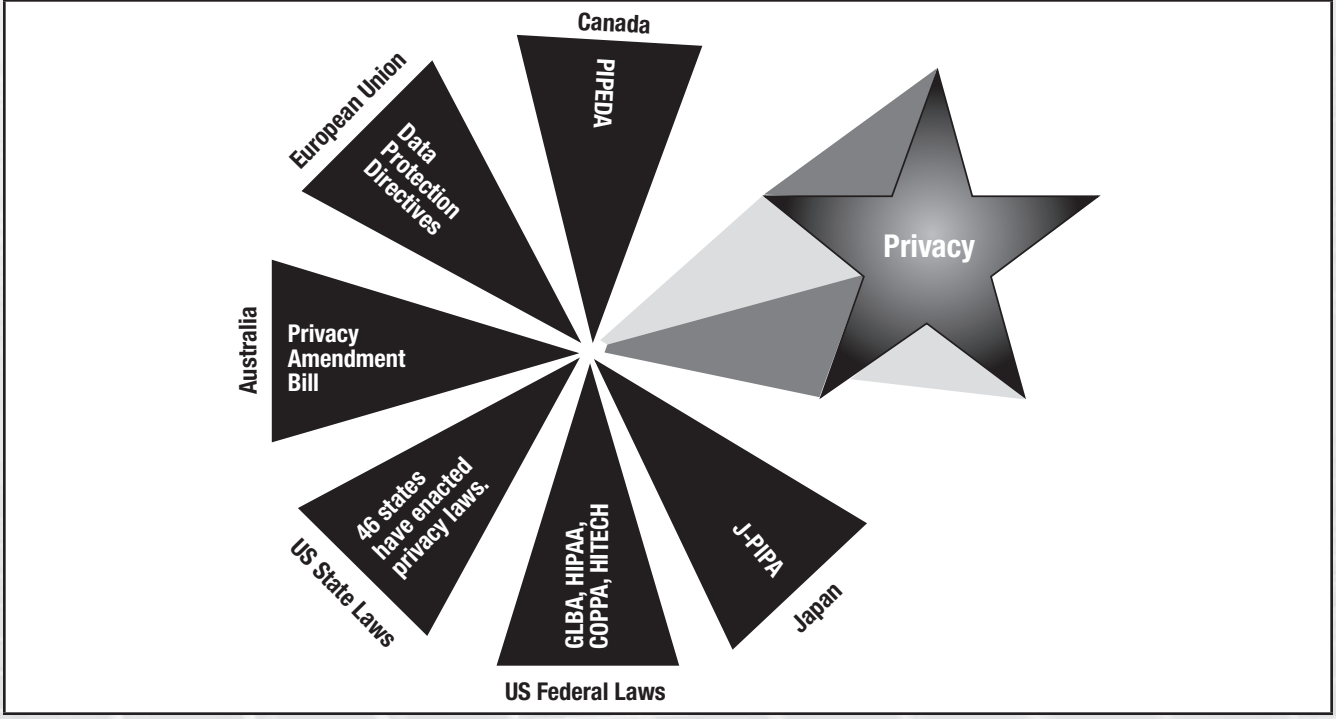
THE VALUE PROPOSITION OF INSTITUTING A HOLISTIC PRIVACY ARCHETYPE

The diverse set of regulations and their nonhomogeneity across regions may make it difficult, if not impossible, for a business to institute an efficient information privacy compliance program.

In addition, most of these regulations are backward-looking and have been promulgated in response to historic events.[2] One has to acknowledge the fact that, as market dynamics change, technology, legal and reputational risks may manifest themselves in new ways or in magnitudes not previously recognized, which would call for a transformation to the regulatory rulebooks.

The importance of maintaining a viable, dynamic and progressive IT privacy management mechanism is beyond dispute among businesses. However, traditional approaches and a piecemeal compliance mind-set cannot absorb the privacy risks indefinitely or be scalable enough to cope with evolving regulatory requirements. A proactive business model would embrace an agenda that recognizes the critical role information privacy plays in the successful realization of business objectives and would transition toward a holistic privacy management archetype.

Figure 1—Privacy Regulations Around the World



UNLEASHING THE HOLISTIC PRIVACY ARCHETYPE

The holistic privacy archetype intends to foster a sound information privacy culture within the institution by reinforcing the enterprise governance discipline through a tiered archetype. The core tiers of the archetype are the business process layer, strategy and governance layer, and operational layer. The operational layer aggregates a three-tiered fabric in itself—the process layer, control layer and component layer. **Figure 2** illustrates the privacy archetype applied to the financial business model. Each tiered layer within the archetype is calibrated to specific, assigned capabilities to ensure that the system as a whole is sufficient to support a successful enterprise privacy agenda. In addition, the model is well positioned to remain aggressive and scalable to the expanding regulatory landscape.

Business Process Layer

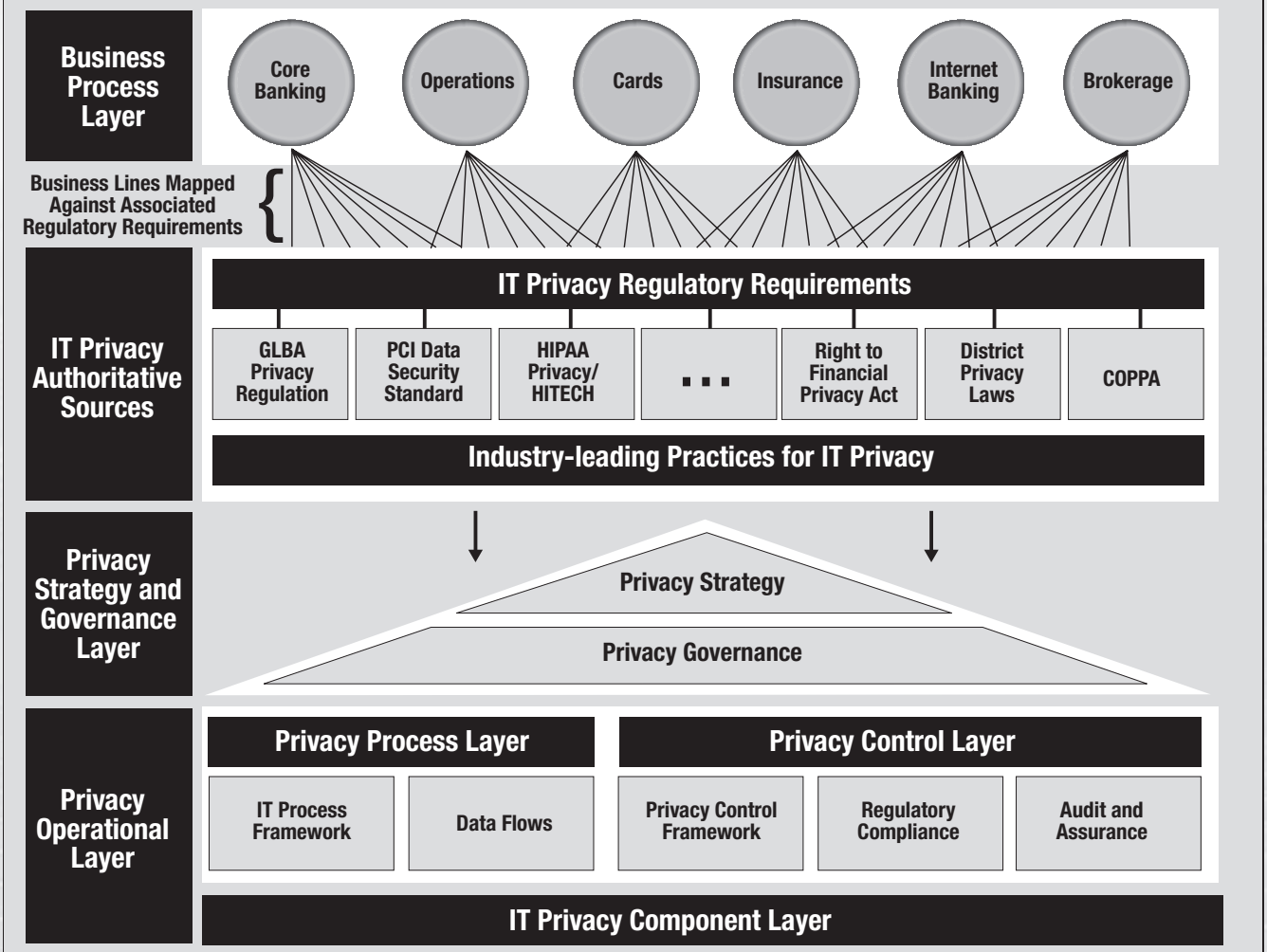
Business processes are a set of coordinated tasks and activities executed by people and technology to accomplish a business service. From a business productivity standpoint, the entity's service portfolio and top-line commitments stem from collective innovations in the business process layer. In addition, the business processes and practices are precisely the focal point in defining the business case for information flow (data collection, data storage, data handling, data sharing and data destruction) within an organization. In other words, the business process layer defines the business case for the collection of information. As the opportunities to use personal data for business grow, enterprises should analyze the adequacy of the underlying controls for managing the evolving risk exposures and strike the right balance between delivering the service customers want and the privacy they expect.

Strategy and Governance Layer

The IT privacy strategy sets the tone and direction for the privacy program, its commitment to information privacy, and the business's overall attitude toward data protection statutes. The layer identifies the enterprise privacy charter and governance objectives and continuously monitors its appropriateness in light of the business's inherent risk exposure resulting from corporate strategic initiatives, reorganizations and process changes.

Privacy governance characterizes a thoughtful balance between accountability and independence among roles to

Figure 2—Application to the Financial Business Model



have clearly drawn lines of authority, limited powers and appropriate controls conducive to legislative, regulatory and industry-leading practices in managing information as an enterprise asset. Privacy governance involves many players—each with specific, assigned responsibilities—to ensure that the system, as a whole, is sufficient to support the privacy strategy and to ensure effectiveness of internal control. The key players include, but are not limited to, the:

- **Data custodian**, who is responsible for the secured custody of data and executes control over the data definitions to ensure that the data conform to consistent definitions throughout the life cycle (collection, storage, handling, sharing and destruction). The data custodian enforces business rules on information, validates the security over information, approves access requests and maintains currency of access groups.
- **Data steward**, who is responsible for ensuring that the data elements within the organization are in good health in terms of accuracy, completeness and consistency. The data steward performs data validation and monitoring of data (from data entry to data transformation and data consumption) and is, thus, accountable for the quality of data.
- **Data administrator**, who is responsible for executing policies and procedures, such as data backup, data versioning, uploading and downloading data, database administration, and actual set-up of the data

Operational Layer

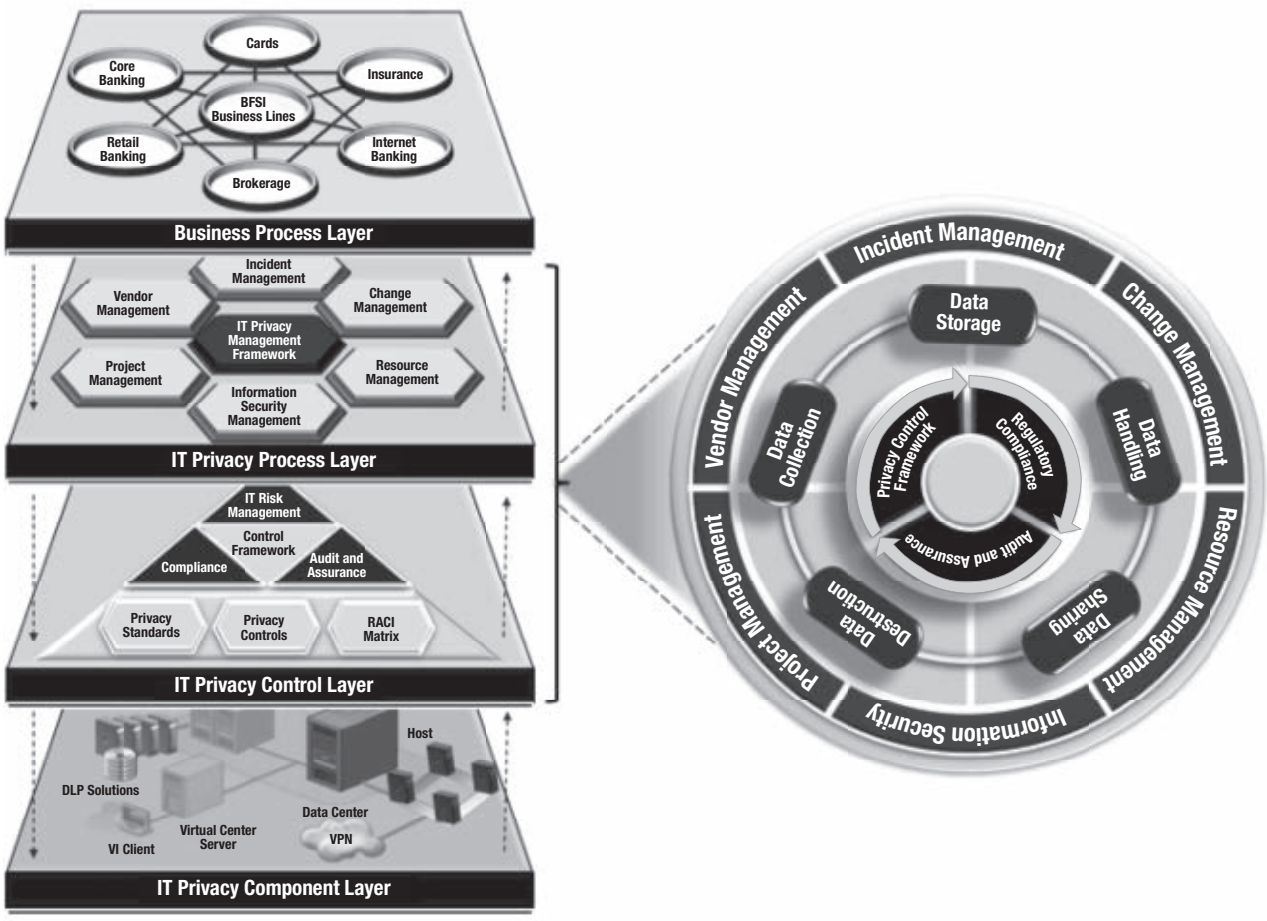
The operational layer is envisaged as the engine that sets a successful privacy system in motion. Dynamic operational practices are the first and strongest line of defense in any information breach scenario. The operational layer compounds three integrated sublayers—the process, control and component layers—which operate in a complementary and mutually reinforcing manner to accomplish the enterprise's privacy objectives. **Figure 3** defines the elements of the operational layer and their integration with business processes.

Process Layer

The process layer sets down definite processes for an enterprise to manage privacy as a service. The layer thereby combines the leading practices of service management (such as those in COBIT, ITIL and ISO 27001) as a means to establish the service framework for information privacy. The belief here is that enterprises choose the processes that best fit their individual strategies:

- **Incident management**—The incident management process offers a consistent mechanism for managing privacy incidents in adherence to regulatory and fiduciary requirements. The incident management process integrates functions such as privacy incident detection, analysis, coordination of appropriate incident response, escalation, communication and notification, event containment, causal analysis, forensic investigation, retention and archival of records, and incident closure. There is always a seamless integration established between the process and the control layers, through mutual handshakes, which is unique to the holistic privacy archetype. As an illustration, the incident management controls underpin the process elements, whereby the process layer establishes the process flows and the control layer defines the statutory obligation elements, such as response timelines and the associated notification requirements specific to the region, to respond to a data breach or privacy incident.
- **Change management**—As business practices and products transform (new services, product sunset, change, etc.), they potentially trigger an associated change to the underlying flow of information. During such occasions, risks may manifest in new ways and in magnitudes not previously recognized, with the potential to create extremely negative

Figure 3—Operational Layer and Business Processes



consequences for sensitive and critical information. It would be imprudent if adequate mitigation controls and strategies are not planned and established before instituting such changes to the operational environment. As a leading practice, the business should reevaluate the risks related to both their conventional and transforming business processes through formal change management processes.

- **Resource management**—Focusing on better resource management practices enhances service effectiveness and streamlines information governance.[3] Assets that are not designed to perform at desired standards and resilience levels pose a significant threat to the information held by the organization. Assets that host personal and/or sensitive information should be validated against architecture baselines and capacity requirements through resource management processes.
- **Information security management**—Information security management establishes definite practices for translating the information governance strategy of an organization into information protection themes and initiatives that are operationally viable. The information security posture of an enterprise demonstrates its strategy toward preventing security breaches and protecting the privacy of its users. Effective management of information security risk requires an enterprisewide approach to ascertain the risks associated with the information handled (i.e., collected, stored, used, transmitted, disposed) by the organization as a reasonable means to balance the legitimate expectations of information privacy against the security levels corresponding to it. From a value-proposition standpoint, the degree of detrimental impact that can result from a serious breach of privacy puts the cost value of information security management into perspective.
- **Project management**—Project management harmonizes adapting and disseminating privacy management processes and controls to a broader array of ongoing and proposed business initiatives. The process fulfills its mandate to supervise and monitor the reliability and soundness of privacy management practices by establishing a privacy project management office. The privacy project management office regulates compliance of the business initiatives handling personal/sensitive information by monitoring whether the project parameters meet their intended privacy goals and by outlining overarching privacy controls through prompt examination of risks.

Enjoying this article?

- Read the ISACA IT Audit and Assurance Guideline G31 Privacy

www.isaca.org/standards

- Access the Privacy and Data Protection topic in ISACA's Knowledge Center

www.isaca.org/knowledgecenter

- **Vendor management**—Outsourcing has transformed over the years, and now includes utility-based service provisioning, managed services, multisourcing, captive centers, conventional outsourcing, cloud computing and much more. From a privacy standpoint, projects managed by third-party vendors pose potential challenges, such as assumption of information management responsibilities outside the control of the source organization. The potential legal liability that may compromise the source organization's dynamics and its privacy track record in terms of breaches would call for a robust privacy control mechanism for third-party vendors. The elements that are essential for enabling a lawful global outsourcing agenda (binding corporate rules, multiparty contracts, vendor monitoring and assurance, etc.) have to be ascertained while establishing the vendor relationship.

Control Layer

The control layer safeguards the long-term best interest of the privacy program by establishing controls to address any control weaknesses and promote compliance with laws and industry-leading practices, governance portfolios, and risk management strategies. The key elements of the control layer include:

- **Risk management**—Management of IT risks begins with conducting a privacy impact assessment to spot potential concentrations of exposures by stratifying the enterprise service portfolio into segments that have common risk characteristics. The critical success element to accomplish a rigorous privacy risk management practice is to reexamine the internal and external environment exposure covenants with respect to the level and nature of information handled by the business.

- **Compliance**—Equally important to the control over the identification and management of the risks is a robust internal control framework that enables organizations to maintain compliance with all applicable laws and regulations.
- **Audit and assurance**—A sound privacy practice becomes meaningless if not followed rigorously. The audit and assurance function is responsible for reviewing the effectiveness of the privacy program and thereby ensuring that the process and control components of the privacy archetype remain unbroken.

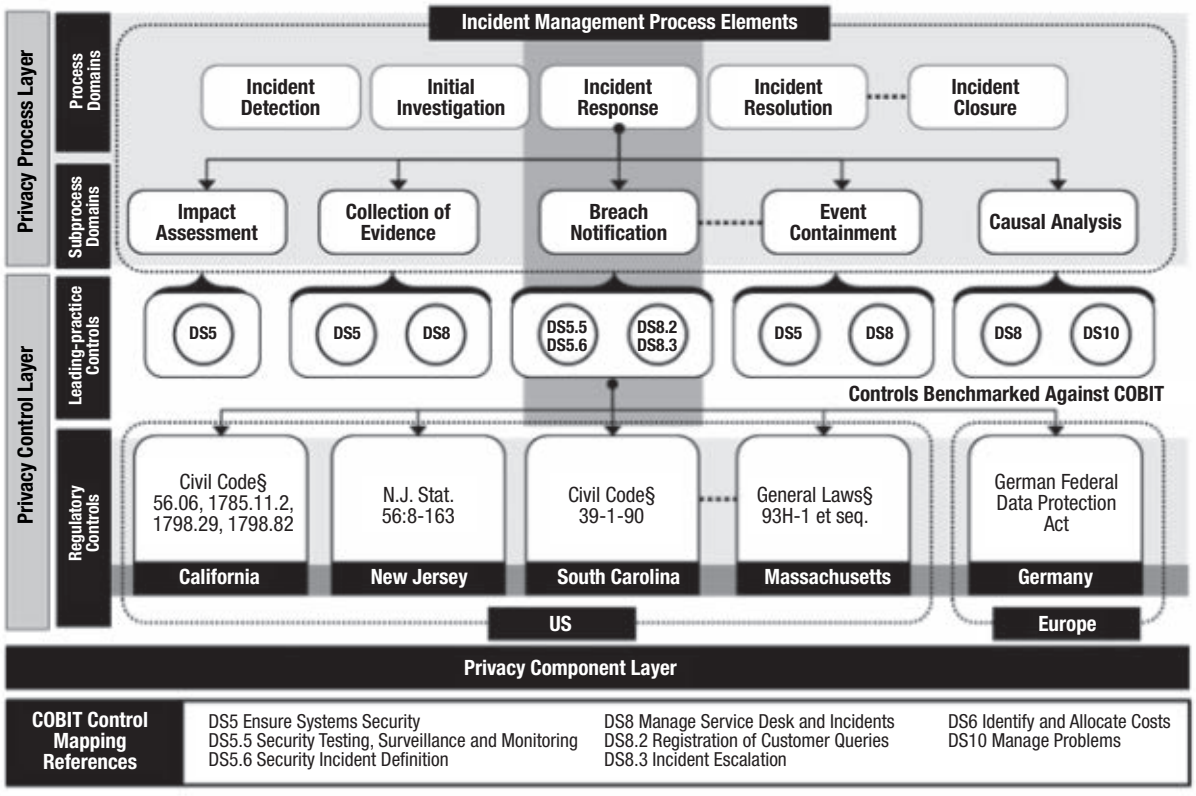
Component Layer

The component layer explores innovative and effective ways to put technology to the best use in supporting privacy and data management functions, and puts in place an infrastructure that can identify, monitor and effectively control the compliance risks. Needless to say, the infrastructure should be commensurate with the nature of the organization's risk profile.

The layer focuses on offering more efficient and effective approaches to streamline data management practices by identifying cost-effective, easy-to-use solutions that are sufficiently robust to aggregate and analyze data across the life cycle:

- **Encryption solution** offers protection of sensitive information from loss and unintentional or deliberate compromise through a process in which data are converted to an unreadable format. The solution enforces security controls over data in motion and/or data at rest based on the enterprise's business dynamics and operational complexity.
- **Data leakage prevention solution** applies data leakage protection parameters over the data at rest and in transit in tune with the corporate privacy strategy by identifying the critical points of sensitive information flow within the business.
- **Data lineage solution** builds the complete data lineage by deducing the chain of source-to-target relationships, thereby establishing data tracking and management

Figure 4—Incident Breach Notification Process



associations on the data source (from where it comes to where it flows and how it is transformed as it travels through the enterprise).

- **Database activity monitoring solution** prevents unauthorized activities by potential hackers, privileged insiders and end users by using policy-based controls and anomaly detection techniques.

EXAMPLE OF THE ARCHETYPE

Figure 4 illustrates the incident breach notification process using the privacy archetype. The value, as discussed throughout this article, is that the archetype provides a reliable, robust, organized and scalable mechanism for managing an enterprisewide privacy program. As the risk factors associated with information accrue and regulatory rule sets deepen, the archetype can endure additions and changes to the respective layers without notably distorting the system as a whole.

CONCLUSION

The market forces aggregate demand and add perspectives for exploring avenues that offset information privacy risks. Exposure of sensitive and personal information and the ever-growing threats to the security of information reveal that privacy of information is of serious concern across all business lines.

These data privacy concerns have renewed the resolve of enterprises across regions and have initiated a broad consensus among market participants to establish a robust privacy management program. However, businesses must recognize that traditional piecemeal approaches in pursuit of this resolve, however well intentioned, may end up redundant, less productive and less able to deliver on the long-term privacy management promise. Reinforcing the need for robust privacy objectives, the proposed privacy archetype focuses on the holistic privacy management paradigm and fosters continual improvement by being flexible to future advances that leading practices and regulations create.

REFERENCES

American Institute of Certified Public Accountants (AICPA), *Generally Accepted Privacy Principles (GAPP)*, USA, 2010

European Union, European Parliament and Council Directive 95/46/EC of 24 October 1995 on "the protection of individuals with regard to the processing of personal data and on the free movement of such data," *http://eur-lex.europa.eu/smartapi/cgi/sga_doc?smartapi!celexplus!prod!DocNumber&lg=en&type_doc=Directive&an_doc=1995&nu_doc=46*

International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC), ISO/IEC 27002:2005, *Information technology—Security techniques—Code of practice for information security management*, Switzerland, 2005

IT Governance Institute, COBIT® 4.1, USA, 2007

National Institute of Standards and Technology (NIST), Special Publication (SP) 800-30, *Risk Management Guide for Information Technology Systems*, USA, 2002

NIST, SP 800-122, *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)*, USA, 2010

Office of Government Commerce (OGC), ITIL Version 3, UK, 2007

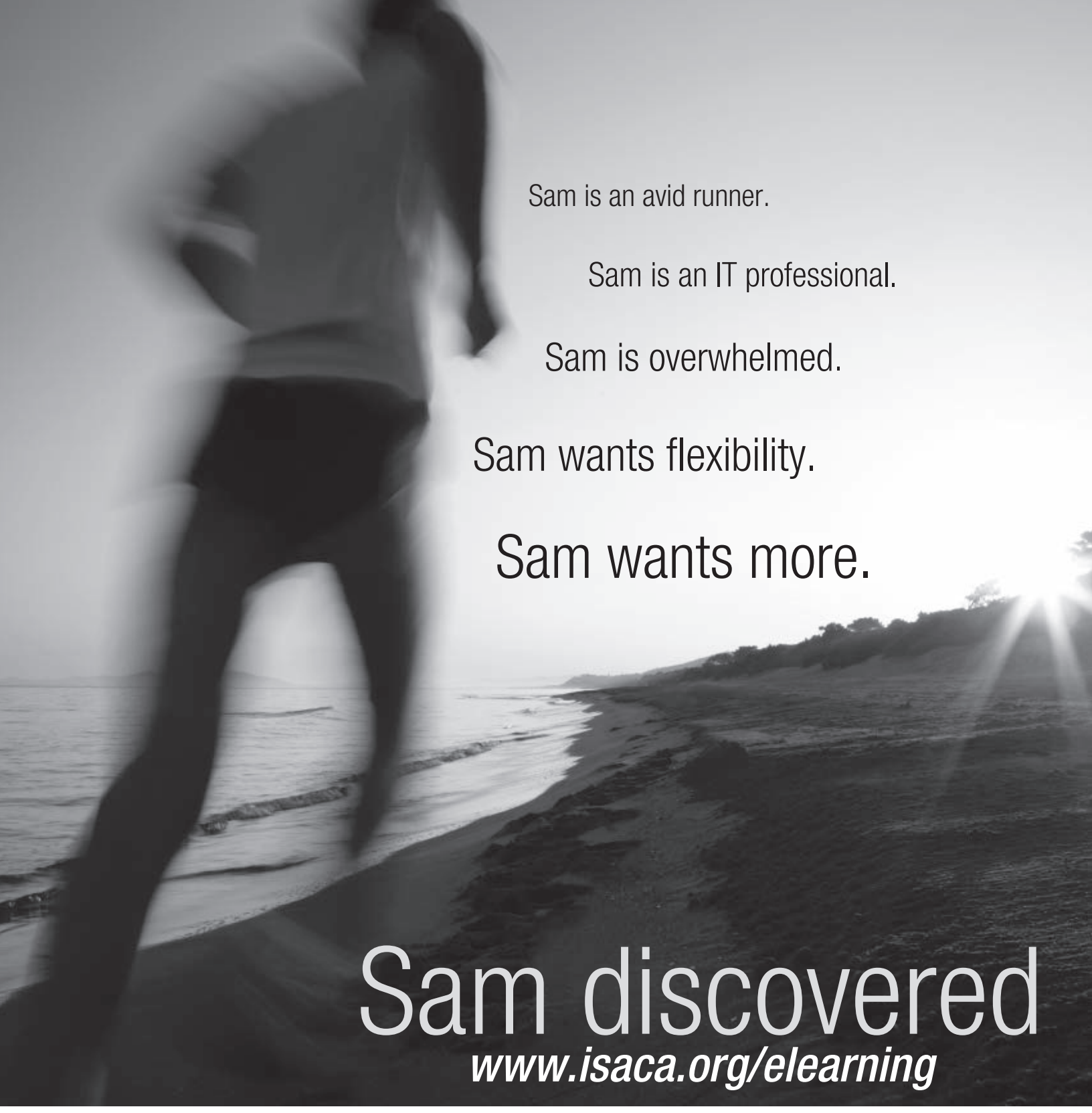
Organization for Economic Co-operation and Development (OECD), *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, France, 1980

ENDNOTES

[1] Greenberg, Andy; "ID Theft: Don't Take It Personally," *Forbes*, 10 February 2010, *www.forbes.com/2010/02/09/banks-consumers-fraud-technology-security-id-theft.html*

[2] Greenspan, Alan; "Bank Regulation," Remarks by Chairman Alan Greenspan before the Independent Community Bankers of America National Convention, 11 March 2005, *www.federalreserve.gov/boarddocs/speeches/2005/20050311*

[3] Office of Government Commerce (OGC), "Service Transition," ITIL Version 3, UK, 2007



Flexibility . . . Knowledge . . . Growth

ISACA®

Trust in, and value from, information systems

Value Assessment Tool for ICT Projects at the European Commission

The Directorate-General for Informatics (DIGIT) enables the European Commission to make effective and efficient use of information and communication technologies to achieve its organisational and political objectives. More than 10 years ago, many European Commission departments, led by the Internal Audit Service and Directorate-General for Agriculture, selected COBIT as a framework for the assessment and improvement of IT processes.

IT governance processes at DIGIT involve strategy and portfolio management, project and development methodology, and enterprise architecture. Major challenges faced by DIGIT today involve improving the integration of business and IT planning cycles as well as optimising investments of scarce resources to maximise the business value of IT.

The Value Assessment Tool (VAST) research is one of many IT governance implementation initiatives led by Francisco Garcia Moran, director general of DIGIT, and Declan Deasy, director of information systems and interoperability solutions. This research takes advantage of frameworks such as ISACA's Val IT and categorises non-financial benefits of projects to highlight and compare their expected value.

When speaking to DIGIT officials about the governance of IT within the Commission, their alignment with ISACA principles and their focus on the five areas of governance that are supported by COBIT are evident.

Georges Ataya, CISA, CISM, CGEIT, CISSP
Academic Director of IT Management Education, Solvay Brussels School of Economics and Management

Stefka Dzhumalieva, a member of the strategy and portfolio management team at the European Commission since 2008, works on enforcing IT governance within the European Commission and steering the development of the e-Commission program. She can be reached at *stefka.dzhumalieva@ec.europa.eu.*

Franck Noëll, was deputy head of the unit and led the strategy and portfolio management team at the European Commission. He is currently head of the IT office at the European Court of Auditors and is responsible for IT governance in the institution. He can be reached at *franck.noel@eca.europa.eu.*

Sébastien Baudu, a member of the strategy and portfolio management team at the European Commission since 2006, works on enforcing IT governance within the European Commission and steering the development of the e-Commission program. He can be reached at *sebastien.baudu@ec.europa.eu.*

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.

Electronic government (e-government) is now mainstream for transforming the public sector so that it achieves its political objectives in an effective, efficient and transparent manner. Today, practically all policy initiatives result in related information and communication technologies (ICT) projects,[1] and ICT has become a key enabler for policy impact, transparency and compliance to norms and standards.

At the same time, public organisations have increasingly limited resources, so new investments have to be made carefully. This trend has been reinforced due to the current economic crisis. Additionally, the complex characteristics of the public sector[2] may further influence new initiatives, so projects could often go beyond their initial scope and budget, and require more time than had been envisaged. They, however, may still be considered successful.

While concepts such as cost-effectiveness and return on investment (ROI) can be easily used to define the success of a project in the private sector, within the public sector the created 'public value' has the biggest weighting.[3] Costly and risky projects must be undertaken to comply with legislative requirements; extended scope is often accepted to satisfy all stakeholders; deadlines are extended to cover all business needs put forward. Therefore, the 'public value' created by an ICT project will determine its success and it should be differentiated from the conventional concepts of project benefits.

Based on similar reflections within the European Commission, the recently set up Corporate Project Office (CPO) had to look for a way to evaluate and prioritise promising ICT projects. Such evaluation needed to distinguish between the public value created by the project (qualitative value) and the cost effectiveness of the project (quantitative value), and at the same time take into account the environment in which this new ICT project would be developed, implemented and operated.

A number of well-established methodologies used in private and public organisations were evaluated for their potential to be reused in the European Commission's context. The analyses concluded that none of the evaluated solutions fit with the specific organisational setup. Therefore, building on these methodologies, the aim was to

define a custom-made, easy-to-use and automated solution, allowing the Commission's services to assess the expected value of envisaged projects. The result of the work is the Value Assessment Tool (VAST) of the European Commission and is the subject of this article.

ICT CONTEXT AT THE EUROPEAN COMMISSION

The European Commission is a complex, decentralised organisation composed of 41 services with a great level of autonomy, each under the leadership of a director-general. This organisational setup is reflected in the ICT aspects of the institution:

- At the business process level, services are fully autonomous and harmonisation is done on an *ad hoc* and voluntary basis.
- At the information systems level, services are also autonomous, but corporate systems are mainly developed by the Directorate-General for Informatics (DIGIT), which is also responsible for defining the development and operating the underlying infrastructure for which certain layers are managed centrally.
- For proximity support services, a consolidation exercise is underway.
- At the infrastructure level, the network, for example, is managed centrally.

DIGIT is also responsible for e-government: internally with the eCommission initiative and with Member States through the Interoperability Solutions for European Public Administrations (ISA) programme.

Like other public administrations, the European Commission is subject to constraints: constant or diminishing resources, in the face of increasing demand. Therefore, priorities have to be carefully established, and the launch of new ICT projects should be based on their expected value. Within the Commission, this aspect is reinforced by the nature of the organisation, since duplications might easily occur when ICT is managed at several, sometimes independent, levels.

To alleviate such difficulties, it is essential to assess the value promised by a given project at an early stage of its inception and, most important, to distinguish between its potential qualitative and quantitative value. It is also important to benefit from a fair comparison element between projects coming from different services. These elements triggered the need for a value assessment methodology.

However, due to the organisational context of the European Commission, such a methodology could not serve its purpose if it was used only at corporate level by the CPO. A potential value assessment methodology needs to be widely adopted by the decentralised structures responsible for ICT. Only suitability to the whole ICT community would reveal the full potential of the selected method.

Therefore, for such a methodology to be accepted, a first requirement is its ease of use and 'self-training'. Qualitative value assessments should take 30 minutes, given the fact that people conducting the assessment have familiarised themselves with the new ICT project through the standard project documentation for the Commission (e.g., business case and vision) or they are part of the project team. The latter case of usage could be defined as self-assessment.

Furthermore, this methodology has to be usable by both ICT and non-ICT professionals so that they can complement each other's views (business and technological) during the project assessment process. Moreover, when decisions have to be taken based on the assessment, the chosen method should provide meaningful, but at the same time, concise, output so that it could be used as a communication means with top management.

Lastly, going beyond the organisational setup and environment, a specific and unique requirement to the Commission is the need to estimate the value of a project at the level of the European Union.

VALUE ASSESSMENT METHODOLOGIES REVIEW

Taking into account the ICT organisational context of the Commission and the specific requirements that it imposed, well-established and practically oriented frameworks/methodologies from both the private and the public sector were selected and examined.

Val IT Framework

Val IT is a governance framework initiated to address the lack of IT investment and management guidelines. Its goal is to ensure the delivery of optimal value from IT investment at adequate costs and levels of risk. The Val IT framework provides extensive guidelines and describes processes to be set up and followed in three main domains: Value Governance, Portfolio Management and Investment Management.[4]

On the positive side, it was considered that Val IT gives a holistic, high-level overview of the mechanisms that can be used to manage the value derived from IT. However, it was not possible to be applied at the European Commission due to the highly decentralised organisational setup when managing ICT. Bearing in mind this constraint, Val IT was used only as an insight for the endeavour.

Demand and Value Assessment Methodology for Better Government Services

The Demand and Value Assessment Methodology for better government services is an initiative of the Australian government that assesses the:

- Demand of e-government services from the viewpoint of end users
- Value of such services, based on the more traditional costs and benefits, but taking into account social and governance implications

It is supported by a spreadsheet-based tool.

The major advantages of the Demand and Value Assessment tool are that it covers both financial and non-financial value and is assisted by a semi-automated tool giving graphical representation of the results. These also closely matched the projects requirements. However, the assessment criteria of the methodology were chosen for the assessment of service provision at the national or local government level and, therefore, differ greatly from those considered at the European level. Furthermore, as it is rather detailed and provides an 'open' structure (criteria and objectives need to be defined by the evaluator), the use of the methodology entailed training, and this was not in line with the aim of easy use and quick results.

Economic Efficiency Assessment Methodology (WiBe) 4.0

WiBe has been used since 1992 by the German federal administration to ensure the economic efficiency of its ICT projects.[6] It is based on two main steps:[7]

1. Identifying parameters that may have an impact on the economic efficiency of the project (a general catalogue of criteria is provided)
2. Determining the economic efficiency of the project with the support of detailed guidelines

The core of WiBe is an exhaustive list of criteria, of which some can be quantified in monetary terms, and some in non-monetary terms. In order to evaluate a project, one should pick the applicable criteria from this catalogue. The strong point of this approach is that it may entail accurate cost/benefit analysis in both monetary and non-monetary terms. However, due to the differences between the chosen criteria, the cross-comparison between projects could be questioned. Again, a disadvantage for the use of this methodology is that it may require up to one day or even more of training if it is used for the first time.[8]

MAREVA

MAREVA was launched in 2005 by the French eGovernment Agency (ADAE) and is widely used by the French governmental organisation, and more recently in Quebec.[9] This methodology bases its assessment on the following axes:[10]

- Profitability
- Risk control
- Values both qualitative and quantitative for the whole public sector
- Values both qualitative and quantitative generated outside of the public sector (citizens and enterprises)
- The project's necessity

MAREVA is composed of two spreadsheet-based files. One addresses the first axis, and the other targets the other four axes. It has been positively evaluated that this approach is structured, and the tool comes with a training package. However, the method focuses on the financial aspects, is greatly detailed, and requires training to understand the various concepts and the calculations. On the contrary, the approach of the European Commission was to focus on the qualitative value.

Value-measuring Methodology

The Value-measuring Methodology (VMM) was developed between 2001 and 2002 under the co-ordination of the Federal Chief Information Officer Council and has the main objective of sound ICT investment management. VMM encompasses four steps:[11]

1. Develop a decision framework.
2. Perform an alternative analysis.
3. Pull the information together.
4. Communicate and document.

This approach is closely linked to the establishment of a business case for new projects and could assist portfolio management practitioners.

The major advantage of this methodology is that it aims to assess both qualitative and quantitative values and builds clear processes to be followed. However, VMM does not propose the set of criteria to be used; it suggests only how to select these criteria and prioritise them to fit the assessed investment closely. While this may entail a close match and precision, the criteria selection process may require time. Further, the cross-comparison between initiatives may be weak if the criteria differ from project to project.

The scope used to evaluate these methodologies has been confirmed by Gartner's report on Public-Value-of-IT Frameworks,[12] in which worldwide examples were selected and reviewed, underlining both their strengths and their weaknesses. Four out of the five assessed methodologies form part of this report.

PROJECT APPROACH

The analyses of the existing methodologies provided a good overview and important insights on the subject of value assessment in the private and public sectors. They have also shown that for such a methodology to serve its purpose, it should be carefully tailored to the environment in which it will be used. However, considering that none of the methodologies fully satisfied the requirements posed by the specific ICT context of the European Commission, a decision was taken to develop a customised solution.

As already explained, the assessment needed to go beyond the traditional financial benefits. Therefore, both qualitative and quantitative criteria had to be used, and the qualitative criteria had to evaluate explicitly the value for the European Union promised by the new project. Furthermore, all ICT projects' assessments should use the same set of criteria to allow cross-comparison and prioritisation. Although keeping its focus on ICT, it should use, as much as possible, business-oriented terms to assure suitability for both business and IT services. Finally, in order to assure effortless adoption, ease of use, and concise and quick presentation of results, a spreadsheet-based tool was selected. Thus, a certain level of automation and enabling flexibility was achieved while the overall approach was still in its adoption phase.

To assure the success of the tool, several iterations of development, tests and feedback sessions with a subset of the European Commission services were completed until a stable version was produced, supported by guidelines for a methodological reference for the use of the tool and for the analyses of the results. The next section of this article looks at the custom-made value assessment tool in more detail.

PRESENTATION OF THE VALUE ASSESSMENT TOOL

VAST is a spreadsheet-based tool that consists of an Index page, five Value perspectives and a graphical Results page (depicted in **figure 1**). The tool is also supported by guidelines that serve as a methodological reference and help its use. Each of these parts is presented in the following sub-sections.

Project Identification

The Index page collects general information about the project: project name, contacts, business owner of the project and date of assessment. This Index page also serves as a central point of the tool, and in doing so, it provides shortcuts to the other parts of the tool.

Value Perspectives

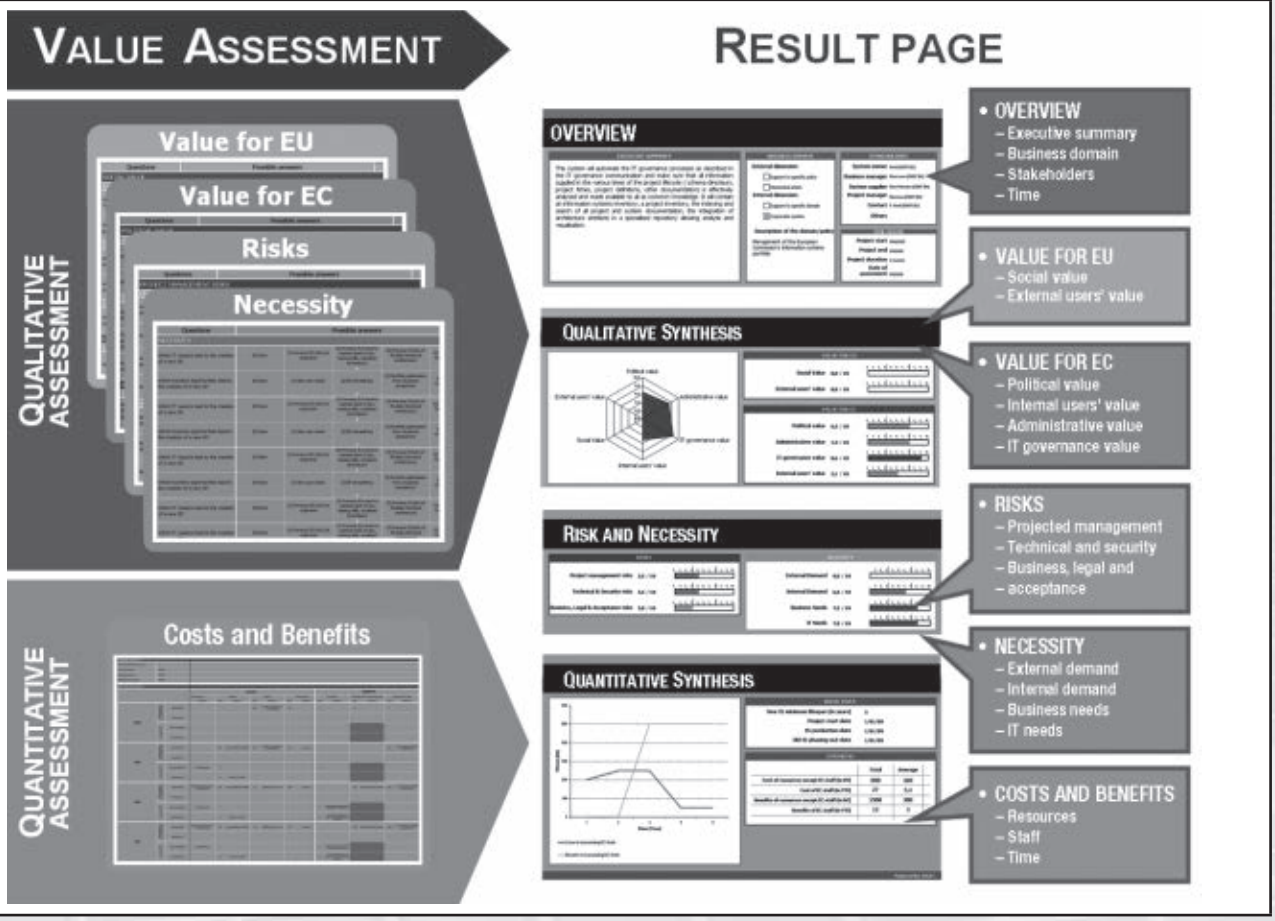
VAST consists of five value perspectives: four estimate the qualitative value of the ICT projects (Value for European Union [EU], Value for European Commission [EC], Risks and Necessity) and one estimates the quantitative value (Financial Costs and Benefits). The four qualitative perspectives consist of sets of criteria that are grouped into a number of sections and sub-sections. The quantitative perspective requires financial information on the project, and some exact figures need to be provided. The five perspectives, with their objectives, are outlined as follows.

The Value for EU perspective looks at the assessment of the external value of an ICT project. Any benefits delivered outside the Commission itself (value to the European society or to European citizens) are considered external value. If the project does not have external users and is used for purely administrative purposes, this value perspective can be omitted.

The Value for EC perspective encompasses criteria that assess the internal value of an ICT project. All factors that can contribute to the improvement of the Commission performance are considered to deliver an internal value, including:

- **Political value**—Whether the IT solution contributes to achieving the Commission's strategic objectives
- **Ad ministrative value**—Whether the project will contribute to the work efficiency and effectiveness

Figure 1—Value Assessment Tool for ICT Projects



- **IT governance value**—Whether the project will contribute to the rationalisation of the Commission's information systems portfolio
- **Internal users' value**—The value for the Commission's employees

The Risks perspective indicates risks related to the need for adequate project management to deliver the ICT project. It also assesses technical, security, business, legal and acceptance-related risks.

The Necessity perspective assesses the need for supporting or developing the project by looking at four subject areas: external demand, internal demand, business needs and technical needs. This perspective tries to answer questions such as 'Do we really need to undertake this project?' and 'Why do we need to support it?'

The Financial Costs and Benefits perspective aims to quantify, in monetary terms, the costs and benefits of the ICT project. The approach consists of identifying every cost for development, maintenance, support, training and infrastructure and the benefits from saved time, reduction in direct operation costs and reduction in IT costs.

Results of the Value Assessment

Each qualitative criterion has a pre-assigned weight (from 1 to 3), which is based on its importance. Furthermore, each criterion has four possible assessments for which it receives between 0 and 3 points multiplied by the criterion weight. This approach promotes both a consistent way of evaluation and fine-tuning and precision of the achieved results. The quantitative criteria are expressed in numbers.

The defined formulas are calculated by the spreadsheet application and are consolidated in the Results page of VAST. The Results page is literally one page (printed) that graphically presents the four qualitative perspectives. The quantitative perspective follows a similar approach and is represented in a different graph.

The assessment is based on the already-provided data. However, to have a complete overview of the project, some supplementary information needs to be introduced into the Results page. This supplementary information is comprised of the project executive summary, the addressed business domain, the main stakeholders and the time frame. Adding this information to the value assessment allows the Results page to be used independently from the tool.

Guidelines

VAST is supported by guidelines that explain each criterion addressed in the five value perspectives. The document lists the criteria in the exact same way as the tool so that a user can easily navigate through it. The guidelines also provide general information on how the tool should be used and how to analyse the achieved results and use the tool as a methodological reference. The guidelines are, thus, entirely sufficient for self-training on VAST.

PRACTICAL APPLICATIONS OF THE VALUE ASSESSMENT TOOL

For an evaluation and validation of the tool, three iterations of development were undertaken. The chosen approach and the set of criteria were presented to the Commission IT community, and the tool was provided for free use by the Commission services. Interested parties were requested to provide detailed feedback from tests undertaken. Building upon these remarks, an adjusted and stable version of the tool was produced. Throughout these iterations, the achievement of the requirements put forward has been confirmed. Some limitations of the tool were also revealed.

The IT professionals at the Commission agreed that it is rather difficult to express in a concise manner the benefits of ICT projects, and they agreed that the VAST tool, which allows qualitative and quantitative value to be distinguished, helps to do this. The VAST tool also sheds light on otherwise overlooked areas of projects. For example, if a system aims at serving needs of the European citizens (external user needs), the spotlight would usually focus on the satisfaction of these needs. However, the project might be using innovative technology or be producing reusable modules. These possibilities additionally increase its value, and VAST can demonstrate this.

Utilising the exact same criteria for each assessment allows a valid cross-comparison of similar projects. For example, VAST can be very useful when the business requests a higher number of projects than what the IT entity can feasibly deliver. The use of the tool allows justified prioritisation, and the projects with higher value can be put forward. However, when comparison needs to be done between projects coming from different services, it is considered best that the evaluation be performed via a mediator (e.g., by the CPO).

The objective for the tool to be suitable for both business and the IT professionals was confirmed by the Health and Consumer Protection policies service. It established a practice to perform value assessment with VAST by representatives from the business and IT at the beginning of a project. Going together through each criterion, discussions identified the weak areas of the project. In this way, many concepts are clarified for the two parties, and a true partnership between business and IT can emerge from this practice.

The results of VAST comprise one self-explanatory page, which gives an overview of not only the qualitative and the quantitative value, but also the risks and necessity of the ICT project. Therefore, the tool can be used for communication purposes to engage senior management and stakeholders of the project. The Results page can be attached to other documentation or can be the subject of a specific meeting. Going even further, as found by the service for Trade Policies, VAST can be considered a helpful management tool.

Overall, it has been confirmed by the Commission services that the tool is easy to use and adopt. A project assessment lasts between approximately 30 minutes and one hour (at first use), assuming that the individuals conducting the assessment have familiarised themselves with the standard project documentation required at the Commission or that they are part of the project team on the business or technology side. It was also confirmed that there is no need for specific training, and where difficulties appear, the guidelines provide a sufficient level of clarification. However, the financial costs and benefits perspective was often noted as challenging to fill in, as concepts like saved time and workload are difficult to express in monetary terms.

Other European institutions (beyond the Commission) also showed interest in adopting VAST. However, as the tool is highly tailored to the Commission context, the adoption requires certain customisation, which has been the case with the European Chemical Agency.

Although this method of internal validation of the tool served its purposes, in order to assess VAST's wider applicability and benefits, a systematic comparison of VAST with similar value frameworks should be conducted.

SUMMARY AND CONCLUSIONS

Public organisations are increasingly managed with limited resources, and decisions for new investments have to be taken cautiously. At the same time, risky and costly projects have to be undertaken due to the circumstances in which such organisations work: compliance with legal regulations, various stakeholders' needs, etc. Thus, costly projects, from a financial perspective, can still bring benefits to public organisations and their stakeholders. This is especially true for the traditionally costly and complex ICT projects.

The public sector requires clear differentiation between the benefits of an ICT project (qualitative value) and its financial cost effectiveness (quantitative value). This work addresses precisely this issue. Building upon the well-established value assessment methodologies, VAST, the Value Assessment Tool of the European Commission, was delivered. To validate the work, three iterations of development were undertaken with the Commission's services, which confirmed the achievement of the tool's requirements and, thus, revealed its benefits: demonstrated value and benefits of ICT projects, cross-comparison and prioritisation, enhanced communication between project stakeholders, suitability for both the business and IT communities, ease of use, and adoptability.

Despite the benefits of VAST, the process of validation also revealed its weak points. It was observed that the financial costs and benefits perspective is challenging to fill in as it is sometimes hard to express in financial terms some of the benefits of a project (e.g., saved time and workload). Further, comparison between projects emanating from different services may be difficult if the assessment is not performed by a mediator, for example the CPO. The tool is highly tailored to the Commission's context, and to be adopted by other organisations, it may require customisation. Finally, the tool has been tested only within the Commission, and to prove its general applicability, further tests should be undertaken. However, as it has been developed in the public domain, the tool package is freely available upon request.

Going beyond the scope of this work, the approach of using a tool for the assessment of important, but intangible areas of ICT management was positively accepted within the European Commission. Using the same approach, a tool for evaluation of the IT governance maturity of the organisation is in its pilot phase.

This article was previously published in *Electronic Government and Electronic Participation: Joint Proceedings of Ongoing Research and Projects of IFIP EGOV and ePart 2010 Conferences* (Trauner, Austria, 2010), edited by Jean-Loup Chappelet, Olivier Glassey, Marijn Janssen, Ann Machintosh, Jochen Scholl, Eftimios Tambouris and Maria A. Wimmer. Permission to republish was granted by the editors of the IFIP EGOV Conference.

The latest version of VAST and its guidelines can be downloaded at *http://ec.europa.eu/dgs/informatics/vast.*

ENDNOTES

1 Schäuble, Wolfgang; 2007, *www.wolfgang-schaeuble.de/fileadmin/user_upload/PDF/070301egovernment.pdf*
2 Rainey, Hal; Robert Backoff; Charles Levine; 'Comparing public and private organizations', *Public Administration Review*, 36/2/1976, p. 233–244
3 Halachmi, Arie; Tony Bovaird; 'Process reengineering in the public sector: learning some private sector lessons', *Technovation*, 5/17/1997, p. 227–235
4 IT Governance Institute, *Enterprise Value: Governance of IT Investments, The Val IT Framework 2.0*, USA, 2006
5 Australian Government, Information Management Office, Demand and Value Assessment Methodology for Better Government Services, Canberra, Australia, 2004
6 ePractice, 2004, *www.epractice.eu/en/library/281229*
7 Federal Ministry of the Interior, Department IT 2 (KBSt), *WiBe 4.0—Recommendations on Economic Efficiency Assessments in the German Federal Administration in Particular with Regard to the Use of Information Technology*, Berlin, 2004
8 *Ibid*.
9 ePractice, 2007, *www.epractice.eu/en/cases/mareva*
10 Le portail du ministère du Budget, des Comptes publics, de la Fonction publique et de la Réforme de l'État, 2007, *https://mioga.minefi.gouv.fr/DB/public/controlegestion/web/pages/CHAP_4_8_Methode_MAREVA.html*
11 Chief Information Officer Council, 2007, *www.cio.gov/documents/ValueMeasuring_Methodology_HowToGuide_Oct_2002.pdf*
12 Gartner, Industry Research, 'Worldwide Examples of Public-Value-of-IT Frameworks' (ID Number: G00146056), 2007

Prepare for the **2011** CISA Exams

ORDER NOW—2011 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.

www.isaca.org/elearning

www.isaca.org/cisareview

To order CISA review material for the June/December 2011 exams, visit the ISACA web site at *www.isaca.org/cisabooks* or see pages S1-S8 in this *Journal*.

CISA® Review Manual 2011

ISACA

The *CISA® Review Manual 2011* 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 (IS) audit, assurance, security and control resource available, based on the recently developed 2011 CISA job practice.

The *CISA Review Manual 2011* features a new format. Each of the five chapters has been divided into two sections for focused study. The first section of each chapter contains the definitions and objectives for the five areas, with the corresponding tasks performed by IS auditors and knowledge statements (required to plan, manage and perform IS audits) that are tested on the exam.

Section One is an overview that provides:
- Definitions for the five new 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 Two for each knowledge statement
- Sample practice questions and explanations of the answers
- Suggested resources for further study

Section Two 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 2011* 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 2011 edition has been developed and is organized to assist candidates in understanding essential concepts and studying the following job practice areas:
- The Process of Auditing Information Systems
- Governance and Management of IT
- Information Systems Acquisition, Development and Implementation
- Information Systems Operations, Maintenance and Support
- Protection of Information Assets

CRM-11 English Edition
CRM-11C Chinese Simplified Edition
CRM-11F French Edition
CRM-11I Italian Edition
CRM-11J Japanese Edition
CRM-11S Spanish Edition

CISA® Review Questions, Answers & Explanations Manual 2011

ISACA

The *CISA® Review Questions, Answers & Explanations Manual 2011* consists of 900 multiple-choice study questions that have previously appeared in the *CISA® Review Questions, Answers & Explanations Manual 2010* and the 2010 Supplement. Many questions have been revised or completely rewritten to recognize changes based on the new 2011 CISA job practice, and to 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 2011*.

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-11 English Edition
QAE-11C Chinese Simplified Edition
QAE-11F French Edition
QAE-11G German Edition
QAE-11I Italian Edition
QAE-11J Japanese Edition
QAE-11S Spanish Edition

CISA® Review Questions, Answers & Explanations Manual 2011 Supplement

ISACA

Developed each year, the *CISA® Review Questions, Answers & Explanations Manual 2011 Supplement* is recommended for use when preparing for the 2011 CISA exam. This supplement consists of 100 new sample questions, answers and explanations based on the new 2011 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-11ES English Edition
QAE-11CS Chinese Simplified Edition
QAE-11FS French Edition
QAE-11GS German Edition
QAE-11IS Italian Edition
QAE-11JS Japanese Edition
QAE-11SS Spanish Edition

CISA® Practice Question Database v11

ISACA

The CISA® Practice Question Database v11 combines the *CISA Review Questions, Answers & Explanations Manual 2011* with the CISA Review Questions, Answers & *Explanations Manual 2011 Supplement* into one comprehensive 1,000-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
- Microsoft .net Framework 3.5
- 512 MB RAM or higher
- One hard drive with 250 MB of available space (flash/thumb drives not supported)
- Mouse
- CD-ROM drive

CDB-11 English Edition—CD-ROM
CDB-11W English Edition—Download
CDB-11S Spanish Edition—CD-ROM
CDB-11SW Spanish Edition—Download

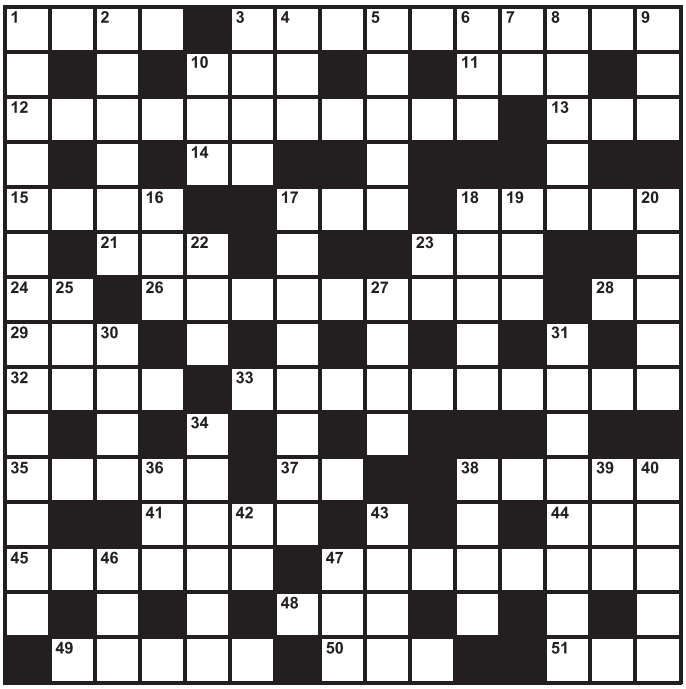
CISA Online Review Course

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 Security investment, abbr.
3 Superior security rating
10 ___ architecture
11 Sign, a deal
12 Risk-averse attitude that legacy security professionals should avoid (three words)
13 Key enabler for policy impact, transparency and compliance
14 You, old way
15 Opinion
17 Middle of the second quarter
18 The European Commission's Directorate-General for Informatics, abbr.
21 Memory
23 Overall software integration for all of the organization's processes (abbr.)
24 Russia's Internet symbol
26 Powerful tools in the risk manager's armory
28 Milliampere, for short
29 Circle segment
32 Image on a radar screen
33 Mobile device that brings a new set of security challenges
35 Smallest
37 Between you and ___
38 RSS for example
41 Seventh Greek letter
44 Admit wrongdoing
45 Examined
47 Security rating for a company that may affect its value when being sold
48 Instigate
49 Director of digital risk and security governance for National Grid, _____ M. Baron
50 Look at
51 Innovative technology dot-com

DOWN
1 Excellent backup guarantees it
2 Problem ____
3 Certain
4 Purpose
5 Half, as a percentage
6 Many ISRM programs were created as part of technology organizations and and are reported on to the ____
7 Buy __
8 Squeezing (out)
9 Add, with up
10 Pay for
16 Functioned as
17 Lowest standards required
18 Sag
19 Internet addresses
20 Follow
22 Hosts
23 Emotional intelligence, for short
25 Web site letters
27 Out of the ordinary
30 Important qualification for an assessor position
31 Predict
34 SSAE 16 for the service auditor changes "audit" to ____
36 Prepared
38 Customer service data, abbr.
39 Pixel maybe
40 Money outlayed
42 Banner, e.g.
43 Innovative
46 The expansion of SAS 70 from AICPA
47 ID info

(Answers on page 54)

Prepare for the **2011** CISM Exams

ORDER NOW—2011 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.

www.isaca.org/cismreview

To order CISM review material for the June/December 2011 exams, visit the ISACA web site at *www.isaca.org/cismbooks* or see pages S1-S8 in this *Journal*.

CISM® Review Manual 2011—*ISACA*

Newly updated, the *CISM Review Manual 2011* 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 been continually enhanced over the past six editions and is a current, comprehensive, peer-reviewed information security management global resource.

The 2011 edition assists helps candidates study and understand essential concepts in the following job practice areas:
- Information security governance
- Information risk management
- Information security program development
- Information security program management
- Incident management and response

The *CISM Review Manual 2011* retains the easy-to-navigate format first introduced in 2010. Each of the book's 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 one of each chapter 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 two for each knowledge statement
- Sample practice questions and explanations of the answers
- Suggested resources for further study

Section two of each chapter consists of reference material and content that support the knowledge statements. The material enhances 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 is effective as a stand-alone document for individual study and as a guide or reference for study groups and chapters conducting local review courses. It is also a primary reference resource for information security managers seeking global guidance on effective approaches to governance, risk management, program development, management and incident response.

CM-11 English Edition **CM-11J** Japanese Edition **CM-11S** Spanish Edition

CISM® Review Questions, Answers & Explanations Manual 2011—*ISACA*

The *CISM Review Questions, Answers & Explanations Manual 2011* compiles 650 multiple-choice study questions that have previously appeared in the *CISM Review Questions, Answers & Explanations Manual 2009*, the *2009 Supplement* and the *2010 Supplement* into one effective resource. These questions are not actual exam items, but are intended to provide the CISM candidate with an understanding of the type and structure of questions and content that have previously appeared on the exam. This publication is ideal to use in conjunction with the *CISM Review Manual 2011.*

To help exam candidates maximize—and customize—their study efforts, questions are presented in the following two ways:
- Job practice area—Questions, answers and explanations are sorted by the current CISM job practice areas. This allows the CISM candidate to refer to questions that focus on a particular area as well as to evaluate comprehension of the topics covered within each practice area.
- Sample 200-question exam—200 of the 650 questions included in the manual are selected to represent a full-length CISM exam, with questions chosen in the same percentages as the current CISM job practice areas. Candidates are urged to use this sample test to simulate an actual exam, but also to determine their strengths and weaknesses in order to identify areas that require further study. Answer sheets and an answer/reference key for the sample exam are also included. All sample test questions have been cross-referenced to the questions sorted by practice area, making it convenient for the user to refer back to the explanations of the correct answers.

CQA-11 English Edition **CQA-11J** Japanese Edition **CQA-11S** Spanish Edition

CISM® Review Questions, Answers & Explanations Manual 2011 Supplements—*ISACA*

Newly created each year, the *CISM Review Questions, Answers & Explanations Manual 2011 Supplement* features 100 new sample questions, answers and explanations to help candidates effectively prepare for the 2011 CISM exam. These new questions are designed to be similar to 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. This publication is ideal to use with the *CISM Review Questions, Answers & Explanations Manual 2011.*

CQA-11ES English Edition **CQA-11JS** Japanese Edition **CQA-11SS** Spanish Edition

CISM® Practice Question Database v11—*ISACA*

The comprehensive CISM Practice Question Database v11 combines the *CISM Review Questions, Answers & Explanations Manual 2011* with the *CISM Review Questions, Answers & Explanations Manual 2011 Supplement* into a single 750-question study guide. Exam candidates can take sample exams with randomly selected questions and view the results by job practice, allowing for concentrated study in particular areas. Additionally, questions generated during a study session are sorted based on 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, giving candidates the ability to customize their study approach to fit their needs. 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; Windows 7
- Microsoft .net Framework 3.5
- 512 MB RAM or higher
- One hard drive with 250 MB of available space (flash/thumb drives not supported)
- Mouse
- CD-ROM drive

MDB-11 English Edition—CD-ROM **MDB-11W** English Edition—Download

An Introduction to ICT Continuity Based on BS 25777

Haris Hamidovic, CIA, ISMS IA, ITIL-F, is chief information security officer at Microcredit Foundation EKI Sarajevo, Bosnia and Herzegovina. Prior to his current assignment, Hamidovic served as IT specialist in the North American Treaty Organization (NATO)-led Stabilization Force (SFOR) in Bosnia and Herzegovina. He is the author of five books and more than 60 articles for business and IT-related publications. Hamidovic is a certified IT expert appointed by the Federal Ministry of Justice of Bosnia and Herzegovina and the Federal Ministry of Physical Planning of Bosnia and Herzegovina.

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.

Organizations have various ways of judging business success. In the public sector, one success criterion is quality of service to the citizens. In the private sector, growth of market share is a success measure. In all sectors, a condition for success is that business should continue to function in the face of fire, flood and other disasters. The discipline that ensures that the business can continue is business continuity management (BCM).[1]

In most organizations, the processes that deliver products and services depend on information and communication technology (ICT). Disruptions to ICT can, therefore, constitute a strategic risk, damaging the organization's ability to operate and undermining its reputation. The consequences of a disruptive incident vary and can be far-reaching, and they may not be immediately obvious at the time of the incident.

In 2008, the British Standards Institution (BSI) released BS 25777:2008, *Information and Communications Technology Continuity Management: Code of Practice*, to help organizations plan and implement an ICT continuity strategy. BS 25777 gives recommendations for ICT continuity management within the framework of BCM provided by BS 25999-1:2006, *Business Continuity Management: Code of Practice*. This article provides an introduction to the key elements of ICT continuity based on BS 25777.

THE CONCEPT OF BUSINESS CONTINUITY

BCM is a relatively new management discipline that has become increasingly important given the turbulent environment in which organizations now find themselves.

The concept of business continuity was developed in the mid-1980s as new way of managing business risks. The basis of BCM is that the key responsibility of company directors is to ensure the continuation of business functionality at all times and under any circumstances.

BCM grew out of requirements in the early 1970s to provide computer disaster recovery for information systems (IS). Traditional disaster planning had concentrated on the restoration of facilities after a major incident such as the loss of a building or plant through fire or flood or the loss of computing or telecommunications throughout an enterprise. Disaster recovery plans, in general, are written on the basis of recovery after an event.

BCM is about prevention—it is not just a cure. It is not only about being able to deal with incidents when they occur and, thus, prevent crisis and subsequent disaster, it is also about establishing a culture within organizations that seeks to build greater resilience to ensure the continuity of product and service delivery to clients and customers.[2]

BCM is focused on entire business processes rather than on particular assets, such as IT systems, because, in order to operate, an organization must continue to execute its critical business processes. These processes may be contained within one business function, or they may integrate or impact a number of them. Recovery of IT systems alone will not keep such business processes running if staff do not have proper working conditions, if critical paper records have been destroyed, or if the organization cannot communicate with its customers and suppliers.[3]

THE CONCEPT OF ICT CONTINUITY

Historically, business continuity planning (BCP) has resided in the IT department of most organizations. For this reason, most companies have some disaster recovery alternatives in place for their IT systems. The most common disaster recovery alternative used is offsite data storage, in which data are regularly backed up to tape or disk and kept at a remote location. Although several other technological alternatives for IT recovery are available, especially for larger

corporations, such as hot and cold sites, electronic vaulting, shadowing, mirroring, and disk-to-disk remote copy, they are not used by many corporations. In this tough economic environment, it is very tempting to cut resources for BCP. Many enterprises mistakenly view BCP as an insurance policy for which they will likely never have to place a claim.[4]

ICT continuity supports the overall BCM process of an organization. BCM seeks to ensure that the organization's processes are protected from disruption and that the organization is able to respond positively and effectively when disruption occurs. The organization sets out its BCM priorities, and within that context, ICT activities take place. ICT continuity ensures that required ICT services are resilient and can be recovered to the predetermined levels within the timescale required and agreed to by top management. Thus, effective BCM depends on ICT continuity to ensure that the organization can meet its objectives at all times (see **figure 1**), particularly during times of disruption.[5]

Figure 1—Relationship Between ICT Continuity and BCM

Source: British Standards Institution, *BS 25777:2008 Information and Communications Technology Continuity Management: Code of Practice*, UK, 2008

THE FOCUS OF ICT CONTINUITY

ICT continuity focuses not only on the likelihood and impact of disruptive incidents, but also on the ability of the organization to detect and respond to the occurrences of such incidents. This requires the organizations to monitor their ICT services to ensure that:[6]

- They are resilient and recoverable at the appropriate level
- Any unexpected event within a service is detected, addressed and investigated in a timely manner
- Dependencies between ICT services and external factors are known and used in assessing risk and the impact of a change
- Dependencies on the technical components are known and used in assessing risk and the impact of change

ICT continuity processes and solutions are also intended to ensure that legal obligations (such as protecting personal and otherwise sensitive data) are not breached.

Enjoying this article?

Access the Business Continuity and Disaster Recover Planning topic in ISACA's Knowledge Center

www.isaca.org/knowledgecenter

PRINCIPLES OF ICT CONTINUITY

ICT continuity is based on six key principles:[7]

1. **Protect**—Protecting the ICT environment from environmental failures, hardware failures, operations errors, malicious attack and natural disasters is critical to maintaining the desired levels of system availability for an organization.
2. **Detect**—Detecting incidents at the earliest opportunity minimizes the impact to services, reduces the recovery efforts and preserves the quality of service.
3. **React**—Reacting to an incident in the most appropriate manner leads to a more efficient recovery and minimizes any downtime. Reacting poorly can result in a minor incident escalating into something more serious.
4. **Recover**—Identifying and implementing the appropriate recovery strategy will ensure the timely resumption of services and maintain the integrity of data. Understanding the recovery priorities allows the most critical services to be reinstated first. Services of a less-critical nature may be reinstated at a later time or, in some circumstances, not at all.

5. **Operate**—Operating in disaster recovery mode until return to normal is possible may require some time and necessitate "scaling up" disaster recovery operations to support increasing business volumes that need to be serviced over time.
6. **Return**—Devising a strategy for every IT continuity plan allows an organization to migrate back from disaster recovery mode to a position in which it can support normal business.

EVALUATING THREATS TO CRITICAL ACTIVITIES

In a BCM context, the level of risk should be understood specifically in respect to the organization's critical activities and the risk of a disruption to these. Critical activities are underpinned by resources such as people, premises, technology, information, supplies and stakeholders. The organization should understand the threats to these resources, the vulnerabilities of each resource, and the impact of a threat if it became an incident and caused a business disruption.

Which risk assessment approach is chosen is entirely the decision of the organization, but it is important that the approach is suitable and appropriate to address all of the organization's requirements.

As a result of a business impact analysis (BIA) and the risk assessment, the organization should identify measures that:

- Reduce the likelihood of a disruption
- Shorten the period of disruption
- Limit the impact of a disruption on the organization's key products and services

These measures are known as loss mitigation and risk treatment. Loss mitigation strategies can be used in conjunction with other options, as not all risks can be prevented or reduced to an acceptable level.[8]

UNDERSTANDING THE ICT REQUIREMENTS FOR BUSINESS CONTINUITY

As part of its BCM program, the organization should categorize its activities according to their priority for recovery. Top management should agree on the organization's business continuity requirements.

For each critical process, the organization needs to determine the longest amount of time the process can be unavailable before that unavailability threatens the survival of the business. This figure is known as the maximum tolerable downtime (MTD).

After the organization sets the MTD for each critical process, it needs to establish some specific recovery objectives for each process. The two primary recovery objectives that organizations set in a BIA are:

1. **Recovery time objective (RTO)**—Target time set for resumption of product, service or activity delivery after an incident
2. **Recovery point objective (RPO)**—Point in time at which data have to be recovered to resume services

The organization should define its ICT services, and ICT service names should be meaningful to the organization.

The ICT services that are required to support achievement of the RTO for each critical activity, as prioritized by the BCM program, should be identified. The organization should document the list of critical ICT services, together with an RTO and RPO for each service. Some indication of the ICT service minimum capacity required at reinstatement and how quickly this capacity may need to be increased could also be necessary. The ICT service RTO should generally be less than the RTO for the critical activity it supports. (This may not be the case when the business continuity strategy calls for an interim measure, such as a manual procedure, instead of depending entirely on the ICT service.)

Top management should agree on the list of critical ICT services and their associated ICT continuity requirements. For each critical ICT service listed and agreed on by top management, the organization should describe and document the ICT components that make up the end-to-end service and how they are configured or linked to deliver each service. This analysis should consider physical and logical configurations. The normal ICT service delivery environment and the ICT continuity service delivery environment configurations should be documented.

The current continuity capability should be reviewed for each critical ICT service, from a prevention perspective, to assess risk of service interruption or degradation (e.g., single points of failure) and to highlight opportunities to improve ICT service resilience and, thus, the likelihood and/or impact of service disruption. It may also highlight opportunities to enable early detection and reaction to ICT service disruption. The organization can decide whether there is a business case to invest in identified opportunities to improve service resilience. This service risk assessment may also advise the business case for enhancing ICT service recovery capability.[9]

IDENTIFYING GAPS

For each critical ICT service, the current ICT continuity service delivery environment configuration should be compared to the normal ICT service delivery environment, from a recovery perspective, to identify gaps or mismatches that may compromise ICT service recovery, such as inadequate data storage capacity.

Gaps identified among critical ICT service continuity capabilities and business continuity requirements should be documented. These gaps may indicate additional resources that each critical ICT service will require during recovery, but that are not already in place.

DETERMINING CHOICES

The organization should consider a range of options for each critical ICT service. The organization may include one or more or all of the following strategies.[10]

Business Continuity

Continuity strategies seek to improve the organization's resilience to a disruption by ensuring critical activities continue at, or are recovered to, an acceptable minimum level and at time frames stipulated within the BIA.

Acceptance

A risk may be acceptable without any further action being taken. Even if it is not acceptable, the ability to do anything about some risks could be limited, or the cost of taking any action could be disproportionate to the potential benefit gained. In these cases, the response may be to tolerate the existing level of risk if top management deems the risk to be acceptable and within the organization's risk appetite. In some circumstances, the impact of a risk may be outside the organization's normal risk appetite, but due to the low likelihood of the risk occurring and/or the uneconomic cost of control, top management may accept the risk.

Transfer

For some risks, the best response may be to transfer them. This may be done by conventional insurance or contractual arrangements, or it may be done by paying a third party to take the risk in another way. Risks may be transferred to reduce the risk exposure of the organization or because another organization is more capable of effectively managing the risks. It is important to note that some risks are not fully transferable; in particular, it is generally not possible to transfer reputational risk, even if the delivery of a service is contracted out.

Change, Suspend or Terminate

In some circumstances, it may be appropriate to change, suspend or terminate the ICT service, product, activity, function or process. This option should be considered only when there is no conflict with the organization's objectives, statutory compliance or stakeholder expectation.

EXERCISING AND TESTING

An organization's ICT continuity plans cannot be considered reliable until exercised. An exercise program may involve a number of tests.

The organization should exercise not only the recovery of the ICT service, but also the service protection and resilience elements to determine whether:

- The service can be protected, maintained and recovered regardless of the incident severity
- The continuity arrangments can minimize the impact to the business

The exercise is a businesswide activity and not just the domain of the ICT department. The ICT department may retain the planning and execution aspects of the exercise, but the organization still has a key role to play.

CONCLUSION

All activity is susceptible to disruption from internal and external events such as technology failure, fire, flood, utility failure, illness and malicious attack. ICT continuity provides the capability to react before a disruption occurs or on detection of one or a series of related events that become incidents, and to respond and recover when those incidents result in disruption.

ICT continuity is integral to ICT strategy and ICT service management, which align to organizational strategy. It is the element of ICT strategy and service management that enables an organization to continue to meet its goals and deliver its products and services when adverse conditions occur.

ICT continuity supports the overall BCM process of an organization. BCM seeks to ensure that the organization's processes are protected from disruption and that the

organization is able to respond positively and effectively when disruption occurs. The organization sets out its BCM priorities, and it is within this context that ICT activities take place.

ICT continuity management and BCM form an important part of effective management, sound governance and organizational prudence. Top management is responsible for maintaining the ability of the organization to continue to function in the face of disruption. Many organizations also have a statutory or regulatory duty to maintain effective risk-based controls, including BCM. BS 25777 will help any organization plan and implement an ICT continuity strategy within the framework of BCM as provided by BS 25999.

ENDNOTES

[1] Her Majesty's Stationery Office (HMSO), *An Introduction to Business Continuity Management*, UK, 1995

[2] Sharp, John; *The Route Map to Business Continuity Management: Meeting the Requirements of BS 25999*, British Standards Institution (BSI), UK, 2007

[3] *Op cit*, HMSO

[4] Rittinghouse, John; James F. Ransome; *Business Continuity and Disaster Recovery for InfoSec Managers*, Elsevier Digital Press, UK, 2005

[5] British Standards Institution, *BS 25777:2008 Information and Communications Technology Continuity Management: Code of Practice*, UK, 2008

[6] *Ibid*.

[7] *Ibid*.

[8] BSI, *BS 25999-1:2006 Business Continuity Management: Code of Practice*, UK, 2006

[9] *Op cit*, BSI, *BS 25777:2008 Information and Communications Technology Continuity Management: Code of Practice*

[10] *Op cit*, BSI, *BS 25999-1:2006 Business Continuity Management: Code of Practice*

ACKNOWLEDGMENT

Permission to reproduce extracts from British Standards is granted by the British Standards Institution (BSI). No other use of this material is permitted. British Standards can be obtained in PDF or hard copy formats from the BSI online shop: *http://shop.bsigroup.com* or by contacting BSI Customer Services for hard copies only: Tel: +44 (0)20 8996 9001, E-mail: *cservices@bsigroup.com.*

2011
ISACA® Training Week

SIX locations . . .
New Orleans, Louisiana, USA…Ottawa, Ontario, Canada…
Seattle, Washington, USA…Minneapolis, Minnesota, USA…
Baltimore, Maryland, USA…Scottsdale, Arizona, USA

FIVE in-depth courses . . .
Fundamentals of IT Audit and Assurance
IT Audit and Assurance Practices
Information Security Management
COBIT®: Strategies for Implementing IT Governance
New! Governance of Enterprise IT

ISACA®
Trust in, and value from, information systems
www.isaca.org/TW2011

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 What should be the guiding principles for determining and reaching agreement on the optimal percentage of operations that ought to be recovered in the event of a contingency by our outsourcing service provider? I am aware of business impact analysis (BIA) and risk assessments (RA) as tools and ways and means to help determine this—both of which I consider to be mere theoretical inputs. From a practical point of view, based on your experience, what should be our approach to determining and reaching agreement on the optimal percentage of business operations that must be or can be recovered in the event of a crisis? In other words, what percentage of the operations must be recovered by the service provider at notional costs, and at what point should the service provider start charging us for continuity arrangements?

A Good questions. While you have said that you are well aware of BIA and RA processes, your question is not clear on a number of things and, hence, I am compelled to make assumptions. You have not said the nature of services that you have outsourced, nor is it clear to me whether you have a single vendor from whom you source the services, or whether you have multiple vendors.

First, let us try to list the guiding principles behind the determination of the optimal percentage of operations that can be recovered at notional costs; of course, the list is not exhaustive:

- **Nature of the business**—This plays an important role in the decision. If the business is something that operates round the clock, 365 days a year, like an online bank, then the need for recovery strategy can be different from that of another company that is engaged in a manufacturing business, for example, in which the production process can wait for a day or two, if circumstances demand. Another important consideration is whether the nature of the internal service includes offering some services to other entities that are dependent on the company's continual functioning.
- **Number of service providers**—Does the organisation have a single service provider that operates from a single location, or is the provider capable of offering services from multiple locations/cities within a country or many countries? Or, does the organisation procure the same services from multiple providers? There can also be scenarios in which multiple providers offer different components of the overall business services.
- **Level of automation**—How people-intensive are the business operations? By people-intensiveness, I mean the quantum of people required to carry out the business processes to meet the business objectives. The more automated the business processes, the less people-intensive the operations become.
- **IT dependency**—Automation and dependency on IT pose different sets of challenges. Availability of systems, applications and processes to carry out the business processes is essential.

Given all of these guiding principles, in an ideal scenario, the service provider may offer to recover approximately 10 to 15 percent of the outsourced operations within about four to six hours at notional cost as part of standard offerings. Anything over and above this may be subject to additional cost. This is the standard offering that I have come across with different service providers.

When the service provider caters to multiple clients from the same facility using a shared infrastructure, recovery operations will be a challenge in terms of prioritising clients. The outsourcing service provider cannot determine the priority for recovery based on the revenue earned from each client. This would mean that the client who has the smallest deal in terms of revenue would be accorded the lowest priority, which is never an acceptable scenario. Every client will be left worried in this scenario because no one wants to be accorded priorities on a relative basis. Buyers of the outsourcing services may always want to be dealt with on absolute terms.

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.

It is true that some clients are more important than other clients, but in general, clients should receive specific services in the event of contingency as per the contract provisions and commitments signed with them originally. Outsourcing service providers normally offer special recovery arrangements in the event of a contingency at an extra cost.

The question in front of us is: How much extra cost should we be prepared to pay to ensure continuity of service arrangements? One of the key benefits of outsourcing is that it results in reduction in costs of internal operations. If so, why spend money to procure services to be delivered in the event of a contingency, if they are not required from a business point of view? This is the point at which the RA and the BIA play a key role. You need to be able to make an informed decision on potential risk scenarios that can be material to your operations.

I cannot prescribe an absolute number—in terms of percentage—for you to consider while determining your recovery arrangements. The trend in the industry, based on my experience and that of my colleagues from whom I sought input, is arrangements in which the vendor realistically restores 10 to 15 percent of the operations immediately. In some instances, it could go up to as much as 25 percent, depending on the industry and the scenario. If someone is promising you 100 percent recovery immediately, there is enough scope to reduce your outsourcing cost by reducing the contingency service arrangements component of the outsourcing package.

NEW ISACA® Certification—CRISC

CRISC™

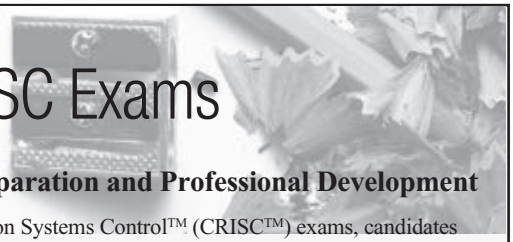
Certified in Risk and Information Systems Control™

An ISACA® Certification

The first exam will take place 11 June 2011.

Visit *www.isaca.org/crisc* for more information.

Prepare for the **2011** CGEIT and CRISC Exams



ORDER NOW—2011 CGEIT and CRISC Review Materials for Exam Preparation and Professional Development

To pass the Certified in the Governance of Enterprise IT® (CGEIT®) and Certified in Risk and Information Systems Control™ (CRISC™) exams, 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 (*www.isaca.org/cgeitreview*).

CGEIT® Review Manual 2011
ISACA

The updated *CGEIT Review Manual 2011* is a detailed reference guide designed to help individuals prepare for the CGEIT exam and understand the roles of those who implement the governance of IT and have significant management, advisory or assurance responsibilities. The manual has been developed and reviewed by subject matter experts actively involved in the governance of IT worldwide.

The 2011 edition includes six chapters devoted to the domains within the scope of the CGEIT job practice:
- IT governance framework
- Strategic alignment
- Value delivery
- Risk management
- Resource management
- Performance measurement

Each chapter features task and knowledge statements with supporting explanations and exhibits detailing their interrelationships. Sample practice questions and explanations of answers assist candidates in effectively preparing for the 2011 CGEIT exam. Also included are definitions of terms typically found on the exam and references for further study.

The manual is an excellent resource for those seeking global guidance and a strong understanding of effective approaches to the governance of IT. It can be used for individual exam study or as a guide for group study. It also serves as a useful desk reference that can be added to the libraries of professionals involved in the governance of IT.

CGM-11 English Edition

CGEIT® Review Questions, Answers & Explanations Manual 2011
ISACA

CGEIT Review Questions, Answers & Explanations Manual 2011 is designed to provide CGEIT candidates with an understanding of the type and structure of questions and content that will appear on the CGEIT exam, the new *CGEIT® Review Questions, Answers & Explanations Manual 2011* consists of 50 multiple-choice study questions. To help candidates maximize study efforts, questions are sorted by domain, allowing CGEIT candidates to focus on particular topics, as well as scrambled as a sample 50-question exam, enabling candidates to effectively determine their strengths and weaknesses and allowing them to simulate an actual exam.

CGQ-11 English Edition

Candidate's Guide to the CGEIT ®Exam and Certification
ISACA

Candidate's Guide to the CGEIT Exam and Certification is supplied to individuals upon receipt of the CGEIT exam registration form and payment. This guide provides a detailed outline of the process and content areas covered on the examination, information on the exam's administration, and a sample copy of the answer sheet used for the exam.

CACG

CGEIT® Certified in the Governance of Enterprise IT® An ISACA® Certification

CRISC™ Review Manual 2011
ISACA

The new *CRISC™ Review Manual 2011* is a comprehensive reference guide designed to help individuals prepare for the CRISC exam and understand IT-related business risk management roles and responsibilities. The 2011 edition has been developed by global subject matter experts to assist candidates in understanding essential concepts of the CRISC job practice areas:
- Risk identification, assessment and evaluation
- Risk response
- Risk monitoring
- IS control design and implementation
- IS control monitoring and maintenance

The *CRISC Review Manual* features a unique learning format for focused study and is separated into two distinct parts.

Part I provides a thorough overview of the concepts related to the IT-related risk management process and the design, implementation, monitoring and maintenance of information systems (IS) controls. Each chapter contains the definitions and objectives for the five CRISC job practice domains, with the corresponding tasks performed by the risk management professional and the knowledge that is tested on the exam. Part I also includes sample practice questions, explanations of the answers and suggested resources for further study.

Part II describes, in detail, selected business and IT processes and how they relate to enterprise risk. For each of the selected processes it:
- Explains the process's importance to achieving business objectives
- Introduces related key concepts
- Provides real-life examples of common risks
- Lists selected key risk indicators
- Describes examples of common IS controls supporting the process
- Features the practitioner's perspective
- Offers suggested reading materials and references

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

CRR-11 English Edition

CRISC™ Review Questions, Answers & Explanations Manual 2011
ISACA

CRISC Review Questions, Answers & Explanations Manual 2011 is designed to provide CRISC candidates with an understanding of the type and structure of questions and content that will appear on the CRISC exam. The new *CRISC Review Questions, Answers & Explanations Manual 2011* consists of 100 multiple-choice study questions. To help candidates maximize study efforts, questions are sorted by domain, allowing CRISC candidates to focus on particular topics, as well as scrambled as a sample 100-question exam, enabling candidates to effectively determine their strengths and weaknesses and allowing them to simulate an actual exam.

CRQ-11 English Edition

Candidate's Guide to the CRISC™ Exam and Certification
ISACA

Candidate's Guide to the CRISC Exam and Certification is supplied to individuals upon receipt of the CRISC exam registration form and payment. This guide provides a detailed outline of the process and content areas covered on the examination, information on the exam's administration, and a sample copy of the answer sheet used for the exam.

CACR

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

ISACA JOURNAL VOLUME 2, 2011 52

CPE Quiz

Prepared by Smita Totade,
Ph.D., CISA, CISM, CGEIT

QUIZ #135

Based on Volume 6, 2010—Challenges of a Changing Landscape

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

TRUE OR FALSE

DUTTA AND KORITALA ARTICLE

1. Many organizations have, or are now in the process of developing, strategies to supplement their manual and costly internal controls with automated, reliable and cost-effective controls and controls solutions to effectively mitigate risk.
2. Controls solutions that focus on only one environment ignore a true enterprise reach, failing to deliver the comprehensive solution to mitigate end-to-end risk.
3. In evaluating the organization's commitment to enhanced products, the following factors need to be considered: the actual amount of revenue invested in product development and the number of major and minor product releases each year, including enhancements and fixes.

SALIDO ARTICLE

4. The proposed approach to data governance for security, privacy, confidentiality and compliance calls for modifying or replacing the organization's existing information security management systems or IT governance processes.
5. Security standards and control frameworks tend to focus primarily on protecting the overall IT infrastructure and on aligning investments in that infrastructure with the organization's business goals.
6. Organizations should place as much emphasis on security and privacy for data that are being transferred as they do for the original data set.
7. Organizations also need to systematically evaluate whether the technologies that protect their data confidentiality, integrity and availability are sufficient to reduce risk to the lowest level.

HAMIDOVIC ARTICLE

8. In Bosnia and Herzegovina, the taxation retention period for the original application for entry into a unified system is 10 years from the date of submission of the application, while the data entered into the database in electronic form have to be kept permanently.
9. Traditionally, corporations have considered the evidentiary implications of electronic documents only when they are required for litigation, or when forensic practitioners have focused on collecting IT evidence as artifacts of an investigation.
10. ISO 15489 may help organizations plan and implement an ICT continuity strategy.
11. One way to proactively address electronic records management is to follow a standardized records management process, such as the one recommended in ISO 27001:2005.

STRAIT ARTICLE

12. Building a business case for a records management initiative begins with providing the description of the scope of the records management initiative, along with details of the future state to be achieved at the end of the initiative.
13. A cross-disciplinary team will aid in collecting the information needed to create a business case for investing in records management.
14. Expanding how and where records management is applied is being recognized as an enabler for reducing storage costs and improving the efficiency of routine operations.

GARBER ARTICLE

15. Audits and separate reviews determine internal control effectiveness continuously.
16. The degree of monitoring key controls may vary based on the relative risk and value of each control.
17. Indirect information such as key performance indicators (KPIs) can provide an excellent source for determining potential indirect monitoring measures.
18. Indirect information can provide positive assurance that a control is operating effectively.

ISACA Journal

CPE Quiz

Based on Volume 6, 2010—Challenges of a Changing Landscape

Quiz #135 Answer Form

(Please print or type)

Name _____

_____

Address _____

_____

_____

CISA, CISM, CGEIT or CRISC# _____

Quiz #135

True or False

DUTTA AND KORITALA ARTICLE

1. _____
2. _____
3. _____

SALIDO ARTICLE

4. _____
5. _____
6. _____
7. _____

HAMIDOVIC ARTICLE

8. _____
9. _____
10. _____
11. _____

STRAIT ARTICLE

12. _____
13. _____
14. _____

GARBER ARTICLE

15. _____
16. _____
17. _____
18. _____

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

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

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

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

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

Call for Articles

for COBIT® Focus

COBIT® Focus is where global professionals share their practical tips for using and implementing ISACA's frameworks

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

IT Governance Institute®

ISACA®

Answers—Crossword by Myles Mellor

See page 43 for the puzzle.

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

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 Effective 16 September 2010
G21 Enterprise Resource Planning (ERP) Systems Review Effective 16 September 2010
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 Effective 1 January 2011

Advertisers/Web Sites

CA technologies	*www.security.com*	Back Cover
CCH Teammate	*www.CCHTeamMate.com*	Inside Back Cover
ExamMatrix	*www.www.ExamMatrix.com/ISJ*	16
Saint®	*www.saintcorporation.com/mac*	1
University of Maryland University College	*www.umuc.edu/cyberedge*	10

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 professionals, entitles one to receive an annual subscription to the *ISACA Journal*.

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

© 2011 ISACA. All rights reserved.

Instructors are permitted to photocopy isolated articles for noncommercial classroom use without fee. For other copying, reprint or republication, permission must be obtained in writing from the association. Where necessary, permission is granted by the copyright owners for those registered with the Copyright Clearance Center (CCC), 27 Congress St., Salem, Mass. 01970, to photocopy articles owned by ISACA, for a flat fee of US $2.50 per article plus 25¢ per page. Send payment to the CCC stating the ISSN (1944-1967), date, volume, and first and last page number of each article. Copying for other than personal use or internal reference, or of articles or columns not owned by the association without express permission of the association or the copyright owner is expressly prohibited.

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

ISSN 1944-1967

Leaders and Supporters

Editor
Deborah Vohasek

Senior Editorial Manager
Jennifer Hajigeorgiou
publication@isaca.org

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

Advertising
The YGS Group
advertising@isaca.org

Media Relations
news@isaca.org

Editorial Reviewers
Matt Altman, CISA, CISM, CGEIT
Brian Barnier, CGEIT
Linda Betz
Pascal A. Bizarro, CISA
Jerome Capirossi, CISA
Cassandra Chasnis, CISA
Ashwin K. Chaudary, CISA, CISM, CGEIT
Joao Coelho, CISA, CGEIT
Reynaldo J. de la Fuente, CISA, CISM, CGEIT
Christos Dimitriadis, Ph.D., CISA, CISM
Ken Doughty, CISA, CBCP
Anuj Goel, Ph.D., CISA, CGEIT, CISSP
Manish Gupta, CISA, CISM, CISSP
Jeffrey Hare, CISA, CPA, CIA
Francisco Igual, CISA, CGEIT, CISSP
Khawaja Javed Faisal, CISA
Romulo Lomparte, CISA, CGEIT
Juan Macias
Norman Marks
David Earl Mills, CISA, CGEIT, MCSE
Robert Moeller, CISA, CISSP, CPA, CSQE
Aureo Monteiro Tavares Da Silva, CISM, CGEIT
Gretchen Myers, CISSP
Daniel Paula, CISA, CISSP, PMP
Pak-Lok Poon, Ph.D., CISA, CSQA, MIEEE
John Pouey, CISA, CISM, CIA
Steve Primost, CISM
Parvathi Ramesh, CISA, CA
David Ramirez
Ron Roy, CISA, CRP
Johannes Tekle, CISA, CIA, CFSA
Ellis Wong, CISA, CFE, CISSP

ISACA Board of Directors (2010–2011):

International President
Emil G. D'Angelo, CISA, CISM

Vice President
Christos Dimitriadis, Ph.D., CISA, CISM

Vice President
Ria T. Lucas, CISA, CGEIT

Vice President
Hitoshi Ota, CISA, CISM, CGEIT, CIA

Vice President
Jose Angel Pena Ibarra, CGEIT

Vice President
Robert E. Stroud, CGEIT

Vice President
Kenneth L. Vander Wal, CISA, CPA

Vice President
Rolf M. von Roessing, CISA, CISM, CGEIT

Past International President, 2007–2009
Lynn Lawton, CISA, FBCS CITP, FCA, FIIA

Past International President, 2005–2007
Everett C. Johnson Jr., CPA

Director
Greg Grocholski, CISA

Director
Tony Hayes, CGEIT

Director
Howard Nicholson, CISA, CGEIT

Chief Executive Officer
Susan M. Caldwell

ISACA Bookstore

Resources for your Professional Development

Over 350 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.

2011 CISA® EXAM REFERENCE MATERIALS

See *www.isaca.org/cisabooks* to prepare for the June or December 2011 CISA exam.

CISA REVIEW MANUAL 2011

CRM-11 English Edition
CRM-11F French Edition
CRM-11I Italian Edition
CRM-11J Japanese Edition
CRM-11S Spanish Edition

CISA REVIEW QUESTIONS, ANSWERS & EXPLANATIONS MANUAL 2011

QAE-11 English Edition (900 Questions)
QAE-11G German Edition (900 Questions)
QAE-11I Italian Edition (900 Questions)
QAE-11J Japanese Edition (900 Questions)
QAE-11S Spanish Edition (900 Questions)

CISA REVIEW QUESTIONS, ANSWERS & EXPLANATIONS MANUAL 2011 SUPPLEMENT

QAE-11ES English Edition (100 Questions)
QAE-11CS Chinese Simplified Edition (100 Questions)
QAE-11FS French Edition (100 Questions)
QAE-11GS German Edition (100 Questions)
QAE-11IS Italian Edition (100 Questions)
QAE-11JS Japanese Edition (100 Questions)
QAE-11SS Spanish Edition (100 Questions)

CISA PRACTICE QUESTION DATABASE V11

(1,000 Questions)
CDB-11 CD-ROM—English Edition
CDB-11W Download—English Edition
(no shipping charges apply to download)
CDB-11S CD-ROM—Spanish Edition
CDB-11SW 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)

2011 CISM® EXAM REFERENCE MATERIALS

See *www.isaca.org/cismbooks* to prepare for the June or December 2011 CISM exam.

CISM REVIEW MANUAL 2011

CM-11 English Edition
CM-11J Japanese Edition
CM-11S Spanish Edition

CISM REVIEW QUESTIONS, ANSWERS & EXPLANATIONS MANUAL 2011

CQA-11 English Edition (650 Questions)
CQA-11J Japanese Edition (650 Questions)
CQA-11S Spanish Edition (650 Questions)

CISM REVIEW QUESTIONS, ANSWERS & EXPLANATIONS MANUAL 2011 SUPPLEMENT

CQA-11ES English Edition (100 Questions)
CQA-11JS Japanese Edition (100 Questions)
CQA-11SS Spanish Edition (100 Questions)

CISM PRACTICE QUESTION DATABASE V11

(750 Questions)
MDB-11 CD-ROM – English Edition
MDB-11W 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)

2011 CGEIT EXAM REFERENCE MATERIALS

See *www.isaca.org/cgeitbooks* to prepare for the June or December 2011 CGEIT exam.

CGEIT REVIEW MANUAL 2011

CGM-11 English Edition

CGEIT REVIEW QUESTIONS, ANSWERS & EXPLANATIONS MANUAL 2011

CGQ-11 English Edition (60 Questions)

CANDIDATE'S GUIDE TO THE CGEIT EXAM AND CERTIFICATION

CACG (No charge to paid CGEIT exam registrants)

2011 CRISC EXAM REFERENCE MATERIALS

See *www.isaca.org/criscbooks* to prepare for the June or December 2011 CISA exam.

CRISC REVIEW MANUAL 2011

CRR-11 English Edition

CRISC REVIEW QUESTIONS, ANSWERS & EXPLANATIONS MANUAL 2011

CRQ-11 English Edition (100 Questions)

CANDIDATE'S GUIDE TO THE CRISC EXAM AND CERTIFICATION

CACR (No charge to paid CRISC 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

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.

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.

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
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
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
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.

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: PROTECTING DIGITAL RESOURCES
NEW
Robert C. Newman

Today, society is faced with numerous Internet schemes, fraudulent scams and means of identity theft that threaten safety and peace of mind. *Computer Security: Protecting Digital Resources* provides a broad approach to computer-related crime, electronic commerce, corporate networking and Internet security—topics that have become increasingly important as more and more threats are made on the Internet. This book is intended for the average computer user, business professional, government worker and those within the education community with the expectation that readers can learn to use the network with some degree of safety and security. The author places emphasis on the numerous vulnerabilities and threats that are inherent in the Internet. Efforts are made to present techniques and suggestions to avoid identity theft and fraud. 2010, 453 pages **1-JBCS**

ENTERPRISE SECURITY FOR THE EXECUTIVE: SETTING THE TONE FROM THE TOP
NEW
Jennifer L. Bayuk

Firewalls breached. Web sites hacked. Confidential files pilfered. Trucks hijacked. Financials manipulated. Today's security teams routinely face nightmare scenarios of malicious, criminal breaches. Executives may not want to get involved in the nuts and bolts of this crucial work, but there is something essential they can do: set the tone for a serious security culture from the top.

Enterprise Security for the Executives: Setting the Tone From the Top is designed to help business executives become familiar with security concepts and techniques to make sure they are able to manage and support the efforts of their security team. It is the first such work to define the leadership role for executives in any business's security apparatus. 2009, 163 pages. **1-ABES**

GFI NETWORK SECURITY AND PCI COMPLIANCE POWER TOOLS
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
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**

IT AUDITING USING CONTROLS TO PROTECT INFORMATION ASSETS, 2ND EDITION
NEW
Chris Davis, Mike Schiller, Kevin Wheeler

Filled with solid techniques, checklists, forms, coverage of leading-edge tools and systematic procedures for common IT audits, *IT Auditing, 2nd Edition* covers real-life scenarios and fosters the skills necessary for auditing complex IT systems. Fully updated to cover new technology including cloud computing, virtualization and storage, the book provides guidance on creating an effective and value-added internal IT audit function. Information is presented in easy-to-follow sections, allowing you to quickly grasp critical and practical techniques.

This edition contains updated tools and checklists, as well as discussions of key concepts and methods for their effective use. This definitive guide offers a unique combination of how-to information on IT auditing for new auditors and cutting-edge audit techniques for experienced professionals. 2011, 512 pages. **15-MIT2**

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**

IT SECURITY METRICS: A PRACTICAL FRAMEWORK FOR MEASURING SECURITY & PROTECTING DATA
NEW
Lance Hayden

IT Security Metrics provides a comprehensive approach to measuring risks, threats, operational activities and the effectiveness of data protection in your organization. The book explains how to choose and design effective measurement strategies and addresses the data requirements of those strategies. The Security Process Management Framework is introduced and analytical strategies for security metrics data are discussed. Readers are shown how to take a security metrics program and adapt it to a variety of organizational contexts to achieve continuous security improvement over time. Real-world examples of security measurement projects are included in this definitive guide. 2010, 396 pages. **22-MSM**

AUDIT, CONTROL AND SECURITY—SPECIFIC ENVIRONMENTS

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

FRAUD AUDITING AND FORENSIC ACCOUNTING, 4TH EDITION
NEW
Tommie W. Singleton, Aaron J. Singleton

With the responsibility of detecting and preventing fraud falling heavily on the accounting profession, every accountant needs to

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

recognize fraud and learn the tools and strategies necessary to catch it in time. Providing valuable information to those responsible for dealing with prevention and discovery of financial deception, *Fraud Auditing and Forensic Accounting, 4th Edition* helps accountants develop an investigative eye toward both internal and external fraud and provides tips for coping with fraud when it is found to have occurred.

This book includes step-by-step keys to fraud investigation and the most current methods for dealing with financial fraud within the organization. Written by recognized experts in the field of white-collar crime, this fourth edition provides readers, whether beginning forensic accountants or experienced investigators, with industry-tested methods for detecting, investigating and preventing financial schemes.
2010, 317 pages. **88-WFA**

PROTECTING INDUSTRIAL CONTROL SYSTEMS FROM ELECTRONIC THREATS NEW

Joe Weiss

Aimed at both the novice and expert in IT security and industrial control systems (ICS), this book will help readers gain a better understanding of protecting ICSs from electronic threats. Cybersecurity is getting much more attention and SCADA security (supervisory control and data acquisition) is a particularly important part of this field, as are distributed control systems (DCS), programmable logic controllers (PLCs), remote terminal units (RTUs), intelligent electronic devices (IEDs), and all other field controllers, sensors, drives and emission controls that make up the "intelligence" of modern industrial buildings and facilities. 2010, 327 pages. **1-MPPI**

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

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.

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 11g (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.

ADMINISTRACIÓN DE LA SEGURIDAD DE INFORMACIÓN

Manuel Tupia Anticona

2010, 201 págs. **2-TCA**

AUDITORÍA DE TECNOLOGÍAS Y SISTEMAS DE INFORMACIÓN.

Piattini, M. y otros

2008, 732 págs. **3-RAMA**

CISA EXAMINATION REFERENCE MATERIAL

Study aids available in Chinese Simplified, French, German, Italian, Japanese and Spanish for the June or December 2011 CISA exam—see page S5

CISM EXAMINATION REFERENCE MATERIAL

Study aids available in Japanese and Spanish for the June or December 2011 CISM exam—see page S5

COMPUTACIÓN FORENSE: DESCUBRIENDO LOS RASTROS INFORMÁTICOS

Jeimy Cano

2009, 340 págs. **1-AOCF**

GOBIERNO DE LAS TECNOLOGÍAS Y LOS SISTEMAS DE INFORMACIÓN

M. Piattini y F. Hervada

2007, 489 págs. **2-RAMA**

PRINCIPIOS DE AUDITORÍA Y CONTROL DE SISTEMAS DE INFORMACIÓN

Manuel Tupia Anticona

2009, 204 págs. **1-TCA**

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

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.
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**

GRAY HAT HACKING: THE ETHICAL HACKERS HANDBOOK, 3RD EDITION NEW

Allen Harper, Shon Harris, Jonathan Ness, Chris Eagle, Gideon Lenkey, Terron Williams

Featuring in-depth, advanced coverage of vulnerability discovery and reverse engineering, *Gray Hat Hacking, 3rd Edition* provides eight brand-new chapters on the latest ethical hacking techniques. In addition to the new chapters, the rest of the book is updated to address current issues, threats, tools and techniques.

This one-of-a-kind guide offers a comprehensive overview of the hacking landscape and is organized in a progressive manner, first giving an update on the latest developments in hacking-related law, useful to everyone in the security field. Next, the book describes the security testing process and covers useful tools and exploit frameworks. The second section is expanded by explaining social engineering, physical and insider attacks, and the latest trends in hacking (voice over-IP and SCADA attacks). The book then explains, from both a code and machine-level perspective, how exploits work and guides readers through writing simple exploits. Finally, the authors provide a comprehensive description of vulnerability research and reverse engineering. 2011, 720 pages. **4-MGH3**

HACKING EXPOSED WIRELESS: WIRELESS SECURITY SECRETS & SOLUTIONS, 2ND EDITION NEW

Johnny Cache, Joshua Wright, Vincent Liu

Protect wireless systems from crippling attacks using the detailed security information in this comprehensive volume. Thoroughly updated to cover today's established and emerging wireless technologies, *Hacking Exposed Wireless, 2nd Edition* reveals how attackers use readily available and custom tools to target, infiltrate and hijack vulnerable systems. The book discusses the latest developments in Wi-Fi, Bluetooth, ZigBee and DECT hacking, and explains how to perform penetration tests, reinforce WPA protection schemes, mitigate packet injection risk, and lock down Bluetooth and RF devices. Cutting-edge techniques for exploiting Wi-Fi clients, WPA2, cordless phones, Bluetooth pairing and ZigBee encryption are also covered in this fully revised guide. 2010, 512 pages. **17-MHE2**

MOBILE APPLICATION SECURITY NEW

Himanshu Dwivedi, Chris Clark, David Thiel

Implement a systematic approach to security in mobile application development with help from this practical guide. Featuring case studies, code examples and best practices, *Mobile Application Security* details how to protect against vulnerabilities in the latest smartphone and PDA platforms. Maximize isolation, lockdown internal and removable storage, work with sandboxing and signing, and encrypt sensitive user information. Safeguards against viruses, worms, malware and buffer overflow exploits are also covered in this comprehensive resource. 2010, 432 pages. **21-MMS**

NO ROOT FOR YOU: A SERIES OF TUTORIALS, RANTS AND RAVES, AND OTHER RANDOM NUANCES THEREIN NEW

Gordon L. Johnson

Over the years, spoon-fed information on anything that involves network auditing has been rather scarce. This book intends to meet this need, proving that such tasks may be explained in an articulate manner, while still maintaining a proper rapport with the individual. This book speaks in layman's terms, while still maintaining proper terminology and utilizing metaphors to express the idea in a more understandable form. A quick-reference for network auditors, it contains step-by-step, illustrated tutorials, explanations regarding why each exploitation works, and information on how to defend against such attacks. 2008, 424 pages. **1-WCNR**

IT GOVERNANCE AND BUSINESS MANAGEMENT

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

THE BUSINESS MODEL FOR INFORMATION SECURITY NEW

ISACA

The Business Model for Information Security provides an in-depth explanation to a holistic business model that examines security issues from a systems perspective. Explore various media, including journal articles, webcasts and podcasts, to delve into the Business Model for Information Security™ and to learn more about how to have success in the information security field in today's market.

The Business Model for Information Security enables security professionals to examine security from a systems perspective, creating an environment where security can be managed holistically and allowing actual risks to be addressed. 2010, 72 pages. **BMIS**

CIO BEST PRACTICES: ENABLING STRATEGIC VALUE WITH INFORMATION TECHNOLOGY, 2ND EDITION

NEW

Joseph P. Stenzel, Gary Cokins, Karl D. Schubert, Michael H. Hugos

Anyone working in information technology feels the opportunities for creating and enabling lasting value. The chief information officer CIO helps define those opportunities and turn them into realities. Now in a second edition, *CIO Best Practices* is an essential guide offering real-world practices used by CIOs and other IT specialists who have successfully mastered the blend of business and IT responsibilities. For anyone who wants to achieve better returns on their IT investments, *CIO Best Practices, 2nd Edition* presents the leadership skills and competencies required of a CIO addressing comprehensive enterprise strategic frameworks to fully leverage IT resources.

This practical resource provides best practice guidance on the key responsibilities of CIOs and their indispensable executive leadership role in modern enterprises of all sizes and industries. It is the most definitive and important collection of best practices for achieving and exercising strategic IT leadership for CIOs, those who intend to become CIOs and those who want to understand the strategic importance of IT for the entire enterprise. 2010, 360 pages. **54-WCIO2**

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

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**

IMPLEMENTING THE PROJECT MANAGEMENT BALANCED SCORECARD

NEW

Jessica Keyes

Business managers have long known the power of the balanced scorecard in executing corporate strategy. *Implementing the Project Management Balanced Scorecard* shows project managers how they too can use this framework to meet strategic objectives. It supplies valuable insight into the project management process as a whole and contains detailed explanations on how to effectively implement the balanced scorecard to measure and manage performance and projects.

Filled with examples and case histories, the book directly relates the scorecard concept to the major project management steps of determining scope, scheduling, estimation, risk management, procurement and project termination. Complete with a plethora of resources in its appendices and on the accompanying CD, the text includes detailed instructions for developing a measurement program, a full metrics guide, a sample project plan and a set of project management fill-in forms. 2010, 447 pages, **46-CRC**

INFORMATION TECHNOLOGY FOR MANAGEMENT: IMPROVING STRATEGIC AND OPERATIONAL PERFORMANCE, 8TH EDITION

NEW

Efraim Turban, Linda Volonino

A major revision of a highly respected text that has sold more than 250,000 copies, this book teaches that the major role of IT is to provide enterprises with strategic advantage by facilitating problem solving, increasing productivity and quality, improving customer service, enhancing communication and collaboration, and enabling business process restructuring.

By taking a practical, management-oriented approach, the book demonstrates how IT is a critical success factor in enterprise operations and is critical to their survival. Designed for all business majors, this book covers the basic tools and technologies, as well as emphasizing innovative uses of technology. Integrated throughout is how IT, including the use of social computing, mobile computing, the Internet, intranets and changes how business is done in almost all enterprises. 2011, 496 pages. **80-WITM8**

INFORMATION TECHNOLOGY GOVERNANCE AND SERVICE MANAGEMENT: FRAMEWORKS AND ADAPTATIONS

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 GOVERNANCE: A POCKET GUIDE

NEW

Alan Calder

This pocket guide outlines the key drivers for IT governance in the modern global economy, with particular reference to corporate governance requirements and the need for companies to protect their information assets. The guide examines the role of IT governance in the management of strategic and operational risk. It also looks at the most important considerations when setting up an IT governance framework, and introduces the reader to the Calder-Moir IT Governance Framework, which the author helped to create. The approach throughout avoids technical jargon and emphasizes business opportunities and needs. 2007, 52 pages. **4-ITIG**

IT GOVERNANCE: GUIDELINES FOR DIRECTORS

NEW

Alan Calder

Aligning IT with the business is a key objective for boards and executives. Organizations with effective IT governance consistently generate better returns for their shareholders than equivalent organizations with ineffective IT governance, and the directors of companies that effectively govern their IT are significantly less exposed to compliance and shareholder challenges than others. This book links IT governance to today's corporate governance environment and assesses the corporate impact that the convergence of financial, accounting and governance frameworks will have on organizations competing in today's economy. 2005, 170 pages. **3-ITGD**

IT OUTSOURCING CONTRACTS: A LEGAL AND PRACTICAL GUIDE (POCKET GUIDE)

NEW

Jimmy Desai

Outsourcing the IT function looks attractive. It can offer greater flexibility and cost savings, and enable one to focus on the core business. At the same time, outsourcing IT has its problems. It can involve extra risks and hidden costs. The company's relationship with its IT supplier will not just run itself. The relationship will need to be managed to obtain the services the business requires.

Whether outsourcing IT is the right decision for the organization depends on the needs of the business. Finding the best supplier of IT services is not just a matter of the cheapest deal. It is important to use a supplier with real technological expertise that understands the specific requirements of the industry. 2009, 106 pages. **5-ITOC**

MONITORING INTERNAL CONTROL SYSTEMS AND IT

NEW

ISACA

Monitoring Internal Control Systems and IT provides useful guidance and tools for enterprises interested in applying information technology to support and sustain the monitoring of internal control. Guidance is provided for the design and operation of monitoring activities over existing IT controls; however, customization of the provided approaches, reflecting the specific circumstances of each enterprise, is required.

The main goals/aims of this publication are to:
- Complement and expand on the 2009 COSO *Guidance on Monitoring of Internal Controls*
- Emphasize the monitoring of application and IT general controls
- Discuss the use of automation (tools) for increased efficiency and effectiveness of monitoring processes

This publication will be helpful for executives/senior management, business process owners and IT professionals. 2010, 124 pages. **MIC**

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**

THE SERVICE CATALOG

NEW

Mark O'Loughlin

The Service Catalog means many different things to many different people. However most would agree that a catalog that helps customers and users to quickly identify the services they require clearly adds value. In turn this helps organizations identify key services that support business processes, understand the contribution made by those services and manage them appropriately. This well-constructed book provides practical advice and information that will help organizations to understand how to design and develop a service catalog and understand the role that the service catalog performs within the service portfolio. 2010, 256 pages. **13-VH**

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**

WORLD CLASS IT: WHY BUSINESSES SUCCEED WHEN IT TRIUMPHS

NEW

Peter A. High

Technology are around. It is so pervasive that one may not even recognize when interacting with it. Despite this fact, many companies have yet to leverage information technology as a strategic weapon.

What then are information technology executives to do to raise the prominence of their department? In World Class IT, recognized expert in IT strategy Peter High reveals the essential principles IT executives must follow and the order in which they should follow them whether they are at the helm of a high-performing department or one in need of great improvement. 2009, 192 pages. **87-WWC**

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

ISACA Bookstore Price List

2011 CISA® EXAM REFERENCE MATERIALS

◆ *To prepare for the **June or December 2011** CISA exam, order* ◆

Code	Title		Nonmember	Member
CISA Review Manual 2011*				
CRM-11	English Edition		135.00	105.00
CRM-11F	French Edition		135.00	105.00
CRM-11I	Italian Edition		135.00	105.00
CRM-11J	Japanese Edition		135.00	105.00
CRM-11S	Spanish Edition		135.00	105.00
CISA Review Questions, Answers & Explanations Manual 2011*				
QAE-11	English Edition	(900 Questions)	130.00	100.00
QAE-11G	German Edition	(900 Questions)	130.00	100.00
QAE-11I	Italian Edition	(900 Questions)	130.00	100.00
QAE-11J	Japanese Edition	(900 Questions)	130.00	100.00
QAE-11S	Spanish Edition	(900 Questions)	130.00	100.00
CISA Review Questions, Answers & Explanations Manual 2011 Supplement*				
QAE-11CS	Chinese Simplified Edition	(100 Questions)	60.00	40.00
QAE-11ES	English Edition	(100 Questions)	60.00	40.00
QAE-11FS	French Edition	(100 Questions)	60.00	40.00
QAE-11GS	German Edition	(100 Questions)	60.00	40.00
QAE-11IS	Italian Edition	(100 Questions)	60.00	40.00
QAE-11JS	Japanese Edition	(100 Questions)	60.00	40.00
QAE-11SS	Spanish Edition	(100 Questions)	60.00	40.00
CISA Practice Question Database v11 (1,000 Questions)*				
CDB-11	CD-ROM—English Edition		225.00	185.00
CDB-11W	Download—English Edition (no shipping charges apply to download)		225.00	185.00
CDB-11S	CD-ROM—Spanish Edition		225.00	185.00
CDB-11SW	Download—Spanish Edition (no shipping charges apply to download)		225.00	185.00
CAN*	Candidate's Guide to the CISA Exam and Certification (No charge to paid CISA exam registrants)		15.00	5.00

2011 CISM® EXAM REFERENCE MATERIALS

◆ *To prepare for the **June or December 2011** CISM exam, order* ◆

Code	Title		Nonmember	Member
CISM Review Manual 2011*				
CM-11	English Edition		115.00	85.00
CM-11J	Japanese Edition		115.00	85.00
CM-11S	Spanish Edition		115.00	85.00
CISM Review Questions, Answers & Explanations Manual 2011*				
CQA-11	English Edition	(650 Questions)	90.00	70.00
CQA-11J	Japanese Edition	(650 Questions)	90.00	70.00
CQA-11S	Spanish Edition	(650 Questions)	90.00	70.00
CISM Review Questions, Answers & Explanations Manual 2011 Supplement*				
CQA-11ES	English Edition	(100 Questions)	60.00	40.00
CQA-11JS	Japanese Edition	(100 Questions)	60.00	40.00
CQA-11SS	Spanish Edition	(100 Questions)	60.00	40.00
CISM Practice Question Database v11 (750 Questions)*				
MDB-11	CD-ROM – English Edition		160.00	120.00
MDB-11W	Download – English Edition (no shipping charges apply to download)		160.00	120.00
CGC*	Candidate's Guide to the CISM Exam and Certification (No charge to paid CISM exam registrants)		15.00	5.00

2011 CGEIT EXAM REFERENCE MATERIALS

◆ *To prepare for the **June or December 2011** CGEIT exam, order* ◆

Code	Title	Nonmember	Member
CGM-11*	CGEIT Review Manual 2011	115.00	85.00
CGQ-11*	CGEIT Review Questions, Answers & Explanations Manual 2011 English Edition (60 Questions)	60.00	40.00
CACG*	Candidate's Guide to the CGEIT Exam and Certification 2011 (No charge to paid CGEIT exam registrants)	15.00	5.00

2011 CRISC EXAM REFERENCE MATERIALS

◆ *To prepare for the **June or December 2011** CRISC exam, order* ◆

Code	Title	Nonmember	Member
CRR-11*	CRISC Review Manual 2011	115.00	85.00
CRQ-11*	CRISC Review Questions, Answers & Explanations Manual 2011 (100 Questions)	60.00	40.00
CACR*	Candidate's Guide to the CRISC Exam and Certification (No charge to paid CRISC exam registrants)	15.00	5.00

COBIT®

Code	Title	Nonmember	Member
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.** ◀

Code	Title	Nonmember	Member
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	42.00	32.00

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™

Code	Title	Nonmember	Member
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

Code	Title	Nonmember	Member
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	80.00	70.00
27-CRC	Guide to Optimal Operational Risk and Basel II	124.00	114.00
11-CRC8	How to Complete a Risk Assessment in 5 Days or Less	95.00	85.00
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 Management & Risk Assessment	105.00	95.00
55-WRCS	Risks, Controls, and Security: Concepts and Applications	118.00	108.00
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

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

ISACA Bookstore Price List

AUDIT, CONTROL AND SECURITY—ESSENTIALS

Code	Title	Nonmember	Member
1-IT8	Accounting Information Systems, 8th Edition	233.00	223.00
70-WAS	Accounting Information Systems: Controls and Processes	169.00	159.00
6-PAW	Applied Security Visualization	65.00	55.00
45-WAP	Audit Planning: A Risk-Based Approach	80.00	70.00
6-PL	Auditing IT Infrastructures	105.00	95.00
53-WAG	Auditor's Guide to Information Systems Auditing	115.00	105.00
76-WSL	Build Your Own Security Lab: A Field Guide for Network Testing	60.00	50.00
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	140.00	130.00
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
1-JBCS	Computer Security: Protecting Digital Resources	93.00	83.00
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
1-ABES	Enterprise Security for the Executive: Setting the Tone from the Top	45.00	35.00
71-WCF	Essentials of Corporate Fraud	55.00	45.00
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
36-CRC	How to Achieve 27001 Certification: An Example of Applied Compliance Management	100.00	90.00
2-W404	How to Comply with Sarbanes-Oxley Section 404: Assessing the Effectiveness of Internal Control, 3rd Edition	95.00	85.00
7-ART	Implementing the ISO/IEC 27001 Information Security Management System Standard	105.00	95.00
9-CRC	Information Security Architecture: An Integrated Approach to Security in the Organization, 2nd Edition	100.00	90.00
28-CRC	Information Security: Design, Implementation, Measurement and Compliance	110.00	100.00
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	100.00	90.00
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-MIT2	IT Auditing Using Controls to Protect Information Assets, 2nd Edition	80.00	70.00
	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	7.00	7.00
9-SYN	The IT Regulatory and Standards Compliance Handbook: How to Survive Information Systems Audit and Assessments	83.00	73.00
22-MSM	IT Security Metrics: A Practical Framework for Measuring Security & Protecting Data	60.00	50.00
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	100.00	90.00
1-RIA	Practical IT Auditing with current Supplement	420.00	410.00
75-WSO	The Sarbanes-Oxley Section 404 Implementation Toolkit: Practice Aids for Managers and Auditors, 2nd Edition	100.00	90.00
1-IGI	Securing the Information Infrastructure	110.00	100.00
5-PSM	Security Metrics: Replacing Fear, Uncertainty, and Doubt	70.00	60.00
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	509.00	499.00
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

Code	Title	Nonmember	Member
18-MAO	Applied Oracle Security: Developing Secure Database and Middleware Environments	70.00	60.00
4-DC	Audit Guidelines for DB2	80.00	70.00
1-SAPP	COBIT and the Sarbanes-Oxley Act	45.00	35.00
88-WFA	Fraud Auditing and Forensic Accounting, 4th Edition	85.00	75.00
	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
1-MPPI	Protecting Industrial Control Systems from Electronic Threats	70.00	60.00
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	95.00	85.00

NON-ENGLISH RESOURCES

Code	Title	Nonmember	Member
2-TCA	Administración de la Seguridad de Información	55.00	45.00
3-RAMA	Auditoría de Tecnologías y Sistemas de Información	70.00	60.00

CISA Examination Reference Material
Study aids available in Chinese Simplified, French, German, Italian, Japanese and Spanish for the June or December 2011 CISA exam—see page S1

CISM Examination Reference Material
Study aids available in Japanese and Spanish for the June or December 2011 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)

1-TCA	Principios de Auditoría y Control de Sistemas de Información	40.00	30.00
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

Code	Title	Nonmember	Member
19-M24	24 Deadly Sins of Software Security: Programming Flaws and How to Fix Them	60.00	50.00
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	90.00	80.00
4-MGH3	Gray Hat Hacking: The Ethical Hakers Handbook, 3rd Edition	70.00	60.00
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
17-MHE2	Hacking Exposed Wireless: Wireless Security Secrets & Solutions, 2nd Edition	60.00	50.00
29ST-3	The Little Black Book of Computer Security, 2nd Edition	35.00	25.00
21-MMS	Mobile Application Security	60.00	50.00
86-WNS	Network Security Bible, 2nd Edition	70.00	60.00

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

ISACA Bookstore Price List

Code	Title	Nonmember	Member
59-WNS	Network Security Fundamentals	80.00	70.00
1-GL	NMAP Network Scanning: The Official NMAP Project Guide to Network Discovery and Security Scanning	60.00	50.00
1-WCNR	No Root for You: A Series of Tutorials, Rants and Raves, and Other Random Nuances Therein	33.00	23.00
56-WPC	Phishing and Countermeasures: Understanding the Increasing Problem of Electronic Identity Theft	105.00	95.00
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	100.00	90.00
1-OSM	Security Monitoring	55.00	45.00
6-EL	XSS Exploits—Cross Site Scripting Attacks and Defense	73.00	63.00

IT GOVERNANCE AND BUSINESS MANAGEMENT

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
61-WBSC	Balanced Scorecard Step-by-Step: Maximizing Performance and Maintaining Results, 2nd Edition	60.00	50.00
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
BMIS*	The Business Model for Information Security	60.00	45.00
41-CRC	Business Resumption Planning, 2nd Edition	108.00	98.00
39-CRC	The Business Value of IT: Managing Risks, Optimizing Performance and Measuring Results	86.00	76.00
54-WCIO2	CIO Best Practices: Enabling Strategic Value with Information Technology, 2nd Edition	75.00	65.00
38-CRC	CISO Leadership: Essential Principles for Success	90.00	80.00
74-WCM	Corporate Management, Governance, and Ethics Best Practices	80.00	70.00
32-CRC	Crisis Management Planning and Execution	90.00	80.00
1-WBC	The Definitive Handbook of Business Continuity Management, 2nd Edition	85.00	75.00
37-CRC	Digital Privacy: Theory, Technologies, and Practices	90.00	80.00
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	97.00	87.00
23-WIT	The Executive's Guide to Information Technology, 2nd Edition	105.00	95.00
10-VH	Foundations of IT Service Management Based on ITIL® V3	66.00	56.00
3-VH	Frameworks for IT Management	66.00	56.00
85-WF101	Fraud 101: Techniques and Strategies for Understanding Fraud, 3rd Edition	60.00	50.00
64-WGRC	Governance, Risk and Compliance Handbook: Technology, Finance, Environmental, and International Guidance and Best Practices	165.00	155.00
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
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	66.00	56.00
46-CRC	Implementing the Project Management Balanced Scorecard	90.00	80.00
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 Managers		
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
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
2-PS	Information Security Roles & Responsibilities Made Easy, Version 2	505.00	495.00
3-IGI	Information Technology Governance and Service Management: Frameworks and Adaptations	205.00	195.00
80-WITM8	Information Technology for Management: Improving Strategic and Operational Performance, 8th Edition	201.00	191.00
81-WIC	Internal Controls Policies and Procedures	90.00	80.00
5-VH	ISO/IEC 20000: A Pocket Guide	33.00	23.00
12-VH	IT Financial Management	66.00	56.00
3-ITGD	IT Governance: Guidelines for Directors	90.00	80.00
4-ITIG	IT Governance: A Pocket Guide	26.00	16.00
WGPM*	IT Governance and Process Maturity (E-Book—purchase online only)	30.00	FREE
5-ITOC	IT Outsourcing Contracts: A Legal and Practical Guide	41.00	31.00
11-VH	IT Outsourcing: Part 1 Contracting the Partner	42.00	32.00
40-CRC	Leading IT Projects: The IT Manager's Guide	96.00	86.00
49-WMG	Manager's Guide to Compliance: Best Practices and Case Studies	80.00	70.00
	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	33.00	23.00
MIC*	Monitoring Internal Control Systems and IT	70.00	55.00
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	73.00	63.00
	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
13-VH	The Service Catalog	66.00	56.00
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
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
87-WWC	World Class IT: Why Businesses Succeed When IT Triumphs	48.00	38.00

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.

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

ISACA® Customer Order Form

Trust in, and value from, information systems

OFFICE USE ONLY

Vol. 2 -11

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

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

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*

Your contact information will be used to fulfill your request, and may also be used by ISACA to send you information about related ISACA goods and services, and other information in which we believe you may be interested. To learn more, please visit *www.isaca.org* and read our Privacy Policy.

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 payable to "ISACA" in US dollars, drawn on US bank.

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

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

Credit Card # _____

Exp. Date _____

Print Cardholder Name _____

Signature of Cardholder _____

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 v11—download.
No shipping charges apply to CISM Practice Question Database v11—download.

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.**

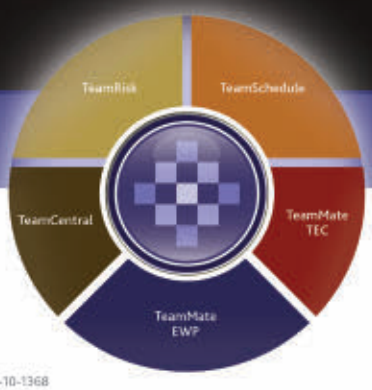
Made my morning coffee.

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



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

who can turn security into "know" instead of "no"?

Saying "no" to unauthorized access is important.
But "know" is far more important.

Content-Aware Identity and Access Management from CA Technologies brings the power of "know" to IT environments—virtual, physical or cloud—all the way down to the data level.

Identities. Access. Information. Compliance.

A smarter, more secure solution.

That's the power of know.

To put the power of know to work for you, visit www.security.com

we can

ca technologies

Copyright ©2011 CA. All rights reserved.