VOLUME 3, 2011

ISACA® Journal

Data Miners

Featured articles:

Every Silver Cloud Has a Dark Lining

Automated Audit Testing for SAP Data

Math on Malware

And more...

ISACA®
Trust in, and value from, information systems

WWW.ISACA.ORG

Grandfathering deadline extended to 30 June 2011!

BALANCE

Risk with Reward

CRISC™ Certified in Risk and Information Systems Control™

An ISACA® Certification

Earn ISACA's Certified in Risk and Information Systems Control™ (CRISC™) designation and gain the rewards of recognition and career advancement. If you've already applied, help contribute to the increasing value of CRISC by encouraging your colleagues to apply for certification.

www.isaca.org/grandfathering

The right balance for your career.

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

Volume 3, 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 June 2011.

An Introduction to Incident Preparedness and Operational Continuity Management Based on ISO/PAS 22399:2007
Haris Hamidovic, CIA, ISMS IA, ITIL-F, IT Project+,

Book Review: Fraud Auditing and Forensic Accounting, 4th Edition
Reviewed by Horst Karin, Ph.D., CISA, CISSP, ITIL

Top IT Governance Issues of 2011
Larry Marks, CISA, CGEIT, CRISC, CFE, CISSP, PMP

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

Join ISACA's LinkedIn group: ISACA (Official), *http://www.linkedin.com/groups/ISACA-Official-3839870*

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

Who Pays for Security?

Steven J. Ross, CISA, CISSP, MBCP, is executive principal of Risk Masters Inc. Ross has been writing one of the *Journal*'s most popular columns since 1998. He can be reached at *stross@riskmastersinc.com.*

In my last article, I raised the issue of the value of information security. I suggested that there were a number of ways to address the issue and that companies ought to place a monetary value on their security preparations. I proposed a thought experiment in which the price for selling a company was dependent in part on the state of its security. One conclusion to be drawn from that experiment is that the value of anything, security in this instance, is what someone will pay for it. In that case, given a certain level of security over information resources in an organization, who is paying for it in any given organization?

At the highest level, of course, shareholders are paying for it in private companies, as are taxpayers in public sector organizations. This is accurate but uninformative. The way in which organizations allocate finite resources says a great deal about how they value the objectives of those internal investments. Some funds go to production, some to sales, some to information technology and some to controls, of which security is a significant part. However, it would be foolish to think that the budgets for production, sales or IT do not also include funds for controls, which are pervasive across an organization. How much, then, of the annual expenditure for each business function includes spending on security? Is the cost evenly distributed? How does each affected organizational unit pay its share for security?

THE INFORMATION SECURITY FUNCTION

What, then, goes into the cost of information security? Essentially, costs are incurred for personnel, hardware, software and services. These categories figure into the budget of the Information Security[1] function. In addition to the salary of dedicated security professionals, generally the function's budget (often subsumed into that of IT) goes toward encryption, access management, intrusion detection and prevention, passwords, firewalls, and penetration testing, to give a few examples. Thus, it may be said that the budget of the Information Security function is the total outlay for a company's security.

But this statement overlooks two very important matters. First, these are not the totality of security expenditures. There are security activities embedded in nearly every business function and there are other functions besides Information Security that perform explicit security roles. Moreover, there is much information in the form of paper records, images and even backup media that is not under the purview of the IT function. Second, the Information Security function is not self-funding. Directly or indirectly, it incurs the cost of security on behalf of the owners of the information and the systems that use it.

ALLOCATION OF RESPONSIBILITY

A portion of the issue of cost is definitional; what in fact does information security consist of? As is often the case, the best (or at least the most widely accepted) answer is to be found in ISO 27002.[2] It divides information security into 11 clauses (often referred to conversationally as domains) (see **figure 1**). Some of these are primarily in the domain of Information Security, but each may involve—even in primary roles—other functions within an organization.

The distribution of responsibilities in **figure 1** is based on a *typical* organization, whatever that means. While any cell within this table may be questioned, the totality of it is indisputable: The Information Security function is a major actor in effecting security but is not always primary in every domain, and in some domains is not involved at all. This is quite clearly stated in ISO 27002: "Information security activities should be coordinated by representatives from different parts of the organization with relevant roles and job functions."[3]

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.

EXPLICIT SECURITY BUDGETING

Thus, it is invalid to say that the cost of security is borne only or even primarily by the Information Security function. It follows that the cost of security is embedded in many budgets across an organization, but it is rare that these costs are explicitly called out in the budgeting process. Therefore, senior management has a poor understanding of what the total cost of security is within its organization, which in turn hinders its ability to make accurate decisions about the adequacy of the investment in protecting information. I am suggesting that the allocations of these costs be clarified.

For example, human resources should identify all the expenditures required for background screening, including salaries, use of investigation agencies, credit checking and

Figure 1—11 Clauses of ISO 27002

Information Security Domains	Primary Responsibility	Typical Security Activities	Other Functions Involved
Security policy	Information security	Policy and standards development and enforcement	Senior policy committee, corporate communications
Organizing information security	Information security	Obtaining management commitment, security coordination, external contacts, independent review	Senior management, corporate communications, internal audit
Asset management	Business function management	Ownership assignment, classification	Information Security, legal
Human resources security	Human resources	Screening, training, removal of access rights	Information Security
Physical and environmental security	Facilities	Securing areas and equipment	Data center operations
Communications and operations management	Data center operations, network operations	Operational procedures, vendor management, system planning and acceptance, network controls	Procurement
Access control	Business function management, information security, individual users	Password management and use, user authentication, network connection control, user identification and authorization, information access restriction	Network operations
Information systems acquisition, development and maintenance	Application development	Security requirements specification, application controls, cryptography, program management, change control	Information Security
Information security incident management	Information security	Reporting and responding to security events	Investigations
Business continuity management	Business continuity management	Risk assessment, developing and maintaining business continuity plans	Information Security
Compliance	Compliance	Complying with laws and regulations, data protection and privacy	Legal, privacy office

whatever else it does in this regard. The percentage of the facilities budget for data center protection should be clearly stated. Business functions should explicitly bear the cost of authorizing their personnel to access information resources and for removing those access rights when a worker is terminated or transferred.

One result will be a diminution of the Information Security function as a cost center. Many of its functions will be charged back to business functions. Information Security's direct role will be to protect the engines of security through such generalized measures as policy, encryption and incident management. By analogy, homeowners and businesses pay for electricity; the power company is responsible for protecting the power plants, which represents a cost that is shared across all customers.

No one can state absolutely what percentage of an organization's operating costs should be attributable to security. The amount will differ among industries and organizations and will be determined ultimately by senior management's appetite for accepting or mitigating risk. Senior management should have a solid understanding of where the organization's investments in security should be made and who within the organization should bear the budgetary burden for those investments.

ENDNOTES

[1] The author has capitalized the term "Information Security" when referring to the function, but not when it refers to the concept.

[2] International Organization for Standardization, ISO/IEC 27002:2005, *Information technology—Security techniques—Code of practice for information security management*, 2005

[3] *Ibid*., p. 10.

IT Audit Basics

Understanding and Applying Benford's Law

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

There are many tools the IT auditor has to apply to various procedures in an IT audit. Almost all computer-assisted audit tools (CAATs)[1] have a command for Benford's Law.[2] This article will attempt to describe what Benford's Law is, when it could apply and what constraints to consider before applying it in an IT audit.

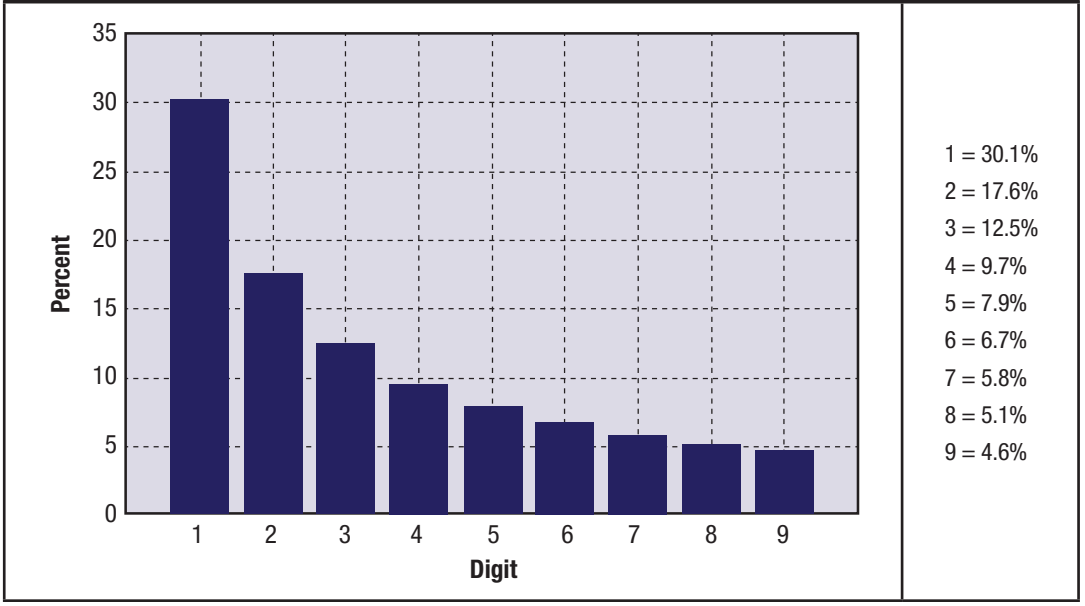
WHAT IS BENFORD'S LAW?

Benford's Law, named for physicist Frank Benford, who worked on the theory in 1938,[3] is the mathematical theory of leading digits. Specifically, in data sets, the leading digit(s) is (are) distributed in a specific, nonuniform way. While one might think that the number 1 would appear as the first digit 11 percent of the time (i.e., one of nine possible numbers), it actually appears about 30 percent of the time (see **figure 1**). Nine, on the other hand, is the first digit less than 5 percent of the time. The theory covers the first digit, second digit, first two digits, last digit and other combinations of digits because the theory is based on a logarithm of probability of occurrence of digits.

Benford's Law holds true for a data set that grows exponentially (e.g., doubles, then doubles again in the same time span), but also appears to hold true for many cases in which an exponential growth pattern is not obvious (e.g., constant growth each month in the number of accounting transactions for a particular cycle). It is best applied to data sets that go across multiple orders of magnitude (e.g., populations of towns or cities, income distributions). While it has been shown to apply in a variety of data sets, not all data sets follow this theory.

The theory does not hold true for data sets in which digits are predisposed to begin with a limited set of digits. For instance, Benford's Law will not hold true for data sets of human heights, human weights and intellectual quotient (IQ) scores. Another example would be small insurance claims (e.g., between US $50 and US $100). The theory also does not hold true when a data set covers only one or two orders of magnitude.

Figure 1—Benford's Law Distribution Leading Digit



WHAT ARE THE RIGHT CIRCUMSTANCES FOR USING BENFORD'S LAW?

Almost from the beginning, proponents of Benford's Law have suggested that it would be a beneficial tool for fraud detection.

A recent example is Mark Nigrini's research, which showed that Benford's Law could be used as an indicator of accounting and expenses fraud.[4] One fraudster wrote numerous checks to himself just below US $100,000 (a policy and procedure threshold), causing digits 7, 8 and 9 to have aberrant percentages of actual occurrence in a Benford's Law analysis. Digital analysis using Benford's Law was also used as evidence of voter fraud in the 2009 Iranian election. In fact, Benford's Law is legally admissible as evidence in the US in criminal cases at the federal, state and local levels. This fact alone substantiates the potential usefulness of using Benford's Law.

Of course the usage of Benford's Law needs to "fit" the audit objective. Some uses are fairly easy to determine for fit. For instance, if the audit objective is to detect fraud in the disbursements cycle, the IT auditor could use Benford's Law to measure the actual occurrence of leading digits in disbursements compared to the digits' probability. Some good examples include thresholds and cutoffs.

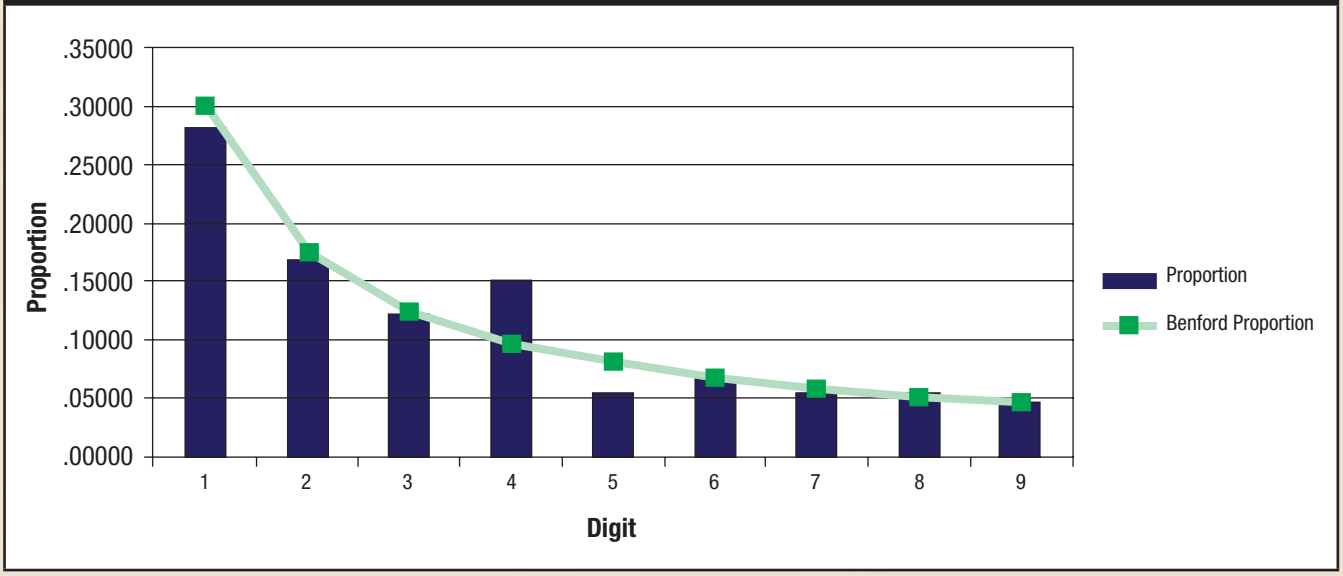
For instance, if a bank's policy is to refer loans at or above US $50,000 to a loan committee, looking just below that approval threshold gives a loan officer the potential to discover loan frauds. If loan fraud was being perpetrated, a Benford's Law test of looking at either the leading digit (specifically, the 4) or two leading digits (specifically, 49) has the potential to uncover the fraud. **Figure 2** shows what a Benford's Law test of the leading digit might show as a result in this particular scenario. The line is Benford's Law probabilities and the bars are the actual occurrences. Note that 4 is aberrantly high in occurrence, and 5 is too low, indicating the possible manipulation of the natural occurrence of loans beginning with 5 (US $50,000 loans) possibly being switched to just under the cutoff or indicating that the suspect could be issuing a lot of $49,999.99 loans fictitiously to embezzle funds.

Another example might be a cutoff of US $2,500 for purchases in which a purchase order is required for any purchase at or above this price point. Thus, a Benford's Law test of the two leading digits (specifically, 24) could reveal any anomalies, manipulation or fraud involving this cutoff. It is also useful as a test of controls to see if existing controls for purchase orders are working effectively. It is important to note that since the cutoff amount has two key digits, a two-digit test is needed rather than a single leading digit.

Other objectives are equally applicable, including analysis of:

- Credit card transactions
- Purchase orders

Figure 2—Benford's Law Test/Comparison



- Loan data
- Customer balances
- Journal entries
- Stock prices
- Accounts payable transactions
- Inventory prices
- Customer refunds

Examples of data sets that are not likely to be suitable for Benford's Law include:

- Airline passenger counts per plane
- Telephone numbers
- Data sets with 500 or fewer transactions
- Data generated by formulas (e.g., YYMM#### as an insurance policy number)
- Data restricted by a maximum or minimum number (e.g., hourly wage rate)

As stated previously, the IT auditor will need to determine whether to run a one-digit test or two-digit test. The two-digit test will usually give more granular results, but is also likely to reveal more spikes than a one-digit test. For certain tests, two digits are critical (see the previous example on purchase order cutoff).

Once the test has been run, the IT auditor will need to determine what results deserve more attention or whether the results provide evidence or information related to the audit objective. Generally speaking, the spikes above the Benford's Law line are the numbers of interest (see 4, not 5, in **figure 2**). The IT auditor will want to obtain independent information on why the digit(s) spike(s). The results that show a digit that is lower than probable occurrence are generally ignored, unless the audit objective is in that direction.

WHAT ARE THE CONSTRAINTS IN USING BENFORD'S LAW?

The assumptions regarding the data to be examined by Benford's Law are:

- Numeric data
- Randomly generated numbers:
  - Not restricted by maximums or minimums
  - Not assigned numbers
- Large sets of data
- Magnitude of orders (e.g., numbers migrate up through 10, 100, 1,000, 10,000, etc.) (Other assumptions exist that are unimportant in applying Benford's Law in IT audits.)

The mathematical theory has always been applied to digital analysis, i.e., a logarithmic study of the occurrence of digits by position in a number.

It is important to note that one assumption of Benford's Law is that the numbers in the large data set are randomly generated. For example, hourly wages will have a minimum and possibly some maximum (even if a realistic maximum) that means that the data set is not generated in a completely random fashion, but rather uses a restricted or manipulated set of digits as the potential leading digit. The same is true if there is a formula or structure to the manner in which the number is generated. For example, US telephone numbers are assigned with a specific area code and a limited number of 3-digit prefaces to the last 4 digits (which are the only truly randomly generated numbers in a phone number). Thus, before applying Benford's Law, the IT auditor should ensure that the numbers are randomly generated without any real or artificial restriction of occurrence.

As can be seen, Benford's Law should be applied only to large data sets. For IT auditors, that would be data such as files with hundreds of transactions (e.g., invoices to customers, disbursements, payments received, inventory items). It is inadvisable to use Benford's Law for small-sized data sets, as it would not be reliable in such cases. Thus, some experts recommend data sets of at least 100 records. This author recommends that the data set be 1,000 records or more, or that the IT auditor justify why a lower volume of transactions is suitable to Benford's Law, i.e., show that the smaller size still meets the other constraints and that size will not affect the reliability of results. The orders of magnitude in particular usually take hundreds of transactions. Using fewer than 1,000 can also lead to too many spikes of interest, too many false positives.

The IT auditor should be careful in extracting a sample and then using Benford's Law on the sample. That is especially true for directed samples in which the amount is part of the factor allowing a transaction to be chosen. This is because the sample is not truly a random sample. For example, pulling a sample of all invoices over US $5,000 leads to a data set that is not random. For small entities, using a data set for the whole month, or a random day of each month, is a better sample for Benford's Law purposes.

CONCLUSION

Benford's Law can recognize the probabilities of highly likely or highly unlikely frequencies of numbers in a data set. The probabilities are based on mathematical logarithms of the occurrence of digits in randomly generated numbers in large data sets. Those who are not aware of this theory and intentionally manipulate numbers (e.g., in a fraud) are susceptible to getting caught by the application of Benford's Law. The IT auditor can also apply Benford's Law in tests of controls and other IT-related tests of data sets. However, the IT auditor needs to remember to make sure that the constraints (mathematical assumptions of the theory) are compatible with the data set to be tested.

ENDNOTES

[1] For an article on using Excel formulas and commands to perform Benford's Law, see: Simkin, Mark G.; "Using Spreadsheets and Benford's Law to Test Accounting Data," *ISACA Journal*, Volume 1, 2010.

[2] Sometimes the command is referred to as "digital analysis."

[3] Actually, Simon Newcomb was the first to posit the leading digits theory in 1881.

[4] Mark J. Nigrini, "I've Got Your Number," *Journal of Accountancy*, May 1999

[5] For more on Benford's Law, especially constraints, see: Hasan, Bassam; "Assessing Data Authenticity with Benford's Law," *Information System Control Journal*, 2002, volume 6.

[6] *Op cit*, Simkin

Five Questions With...

Francisco Garcia Moran

Francisco Garcia Moran started his career as a teacher and IT engineer at the University of Seville (Spain) and worked for several years in the IT departments of the Ministry of Education and Science at the national level and at the Regional Government of Andalusia, where he worked as the head of several IT services.

Since joining the European Commission (EC) in November 1986, Garcia Moran has continued working in the IT area, first at the Informatics Directorate and later at the Directorate-General for Translation.

In 2001, he was appointed director of informatics at the Directorate-General for Personnel and Administration. In this role, Garcia Moran was responsible for the establishment of the Directorate-General for Informatics (DIGIT) in May 2004, and was appointed Director General in November 2005. DIGIT defines the IT strategy of the EC, provides information and communication technology (ICT) corporate services, and is also responsible for the European program Interoperable Solutions for Public Administrations (ISA).

Garcia Moran is a member of the Management Board of the European Network and Information Security Agency (ENISA) and the World Bank's High Level E Transformation Group (HLEG).

Garcia Moran is an avid sports enthusiast. When not in the office, he can be found cycling, playing tennis or basketball, or jogging. He also enjoys reading and classical music.

Q How do you see the role of governance of enterprise IT (GEIT) changing in the next five years?

A I see IT governance being more and more aligned with enterprise governance. Actually, the ultimate goal is that IT governance is completely integrated into enterprise governance since an organization does not have separate IT and business goals, but has business goals with, most of the time, IT components.

In the European Commission (EC), the business has started fully understanding the importance of this alignment, given the fact that the organization relies more and more on IT tools and systems to improve performance, efficiency, effectiveness and compliance and to support European Union (EU) policies. Today, nearly every EU directive or regulation contains provision for the development and implementation of an information system and the associated infrastructure to support the policies. Furthermore, there is some legislation that would be impossible to implement without the support of IT tools.

IT tools are integrated into the business, and given the complexity of interaction among stakeholder organizations, IT governance—and, more globally, governance at all levels—will need to improve a great deal in the coming years.

Q How did major frameworks (e.g., COBIT®, ITIL, ISO 27001) change the landscape of IT management, and what impact did they have on DIGIT?

A The EC uses these frameworks intensively in its IT management and, particularly, in DIGIT in which ITIL, or standard project management methodologies, are systematically deployed.

Furthermore, when carrying out IT audits, these frameworks are used as references. The standard wording at an audit kick-off meeting is, for example:

Audit scope:
The scope of the audit includes the following COBIT processes:
- *DS1 Define and manage service levels.*
- *DS2 Manage third-party services.*
- *ME1 Monitor and evaluate IT performance.*
- *ME3 Ensure compliance with external requirements.*

Audit framework:
- *Regulatory framework at EC*
- *16 internal control standards (baseline requirements as of 1 January 2008),*
- *Legislation (e.g., Regulation 45 (2001) on personal data protection), internal regulation framework (e.g., CEAF, C(2006)3602, SEC(2006)898 & 899).*

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.

Enjoying this article?

- Learn more about and collaborate on Frameworks.

www.isaca.org/knowledgecenter

COBIT:
- *Version 4.1 (May 2007), IT Governance Institute*

ITIL:
- *IT Infrastructure Library for Service Management, version 2 and version 3*

ISO/IEC 27001:
- *ISO/IEC 27001:2005,* Information technology—Security techniques—Information security management systems—Requirements

The Institute of Internal Auditors (The IIA) Research Foundation:
- Global Technology Audit Guide (GTAG) 7: Information Technology Outsourcing

This usage of standard frameworks in audits is, of course, an important incentive to push forward the deployment of these frameworks in IT service and project management within DIGIT and in the whole IT community in the EC and to include these requirements in every IT project.

Q **Are you familiar with other ISACA frameworks, such as Val IT™ and Risk IT? What value do you find in these and other ISACA research projects and publications?**

A Yes, at the EC, we are familiar with these frameworks and they are a source of inspiration and a reference when designing our own tools and methods for internal use. Val IT was an inspiration for VAST, our value assessment tool, and Risk IT is an inspiration for our internal risk assessment.

Q **How do you believe certifications can be useful, and what is their value in Europe and the European public services in particular? What certifications do you look for when hiring new members of your team?**

A Certifications are a good reference for our staff, and we facilitate, as much as possible, our staff becoming certified. For the time being, we are concentrating on IT governance, project management and IT security certifications.

Q **What has been your biggest workplace challenge since you arrived in this position as head of DIGIT, and how did you face it?**

A To give you some background, in the seven years that I have been in my job as senior manager in IT, we have nearly doubled the size of the team (internal staff and consultants). The growth occured because we were trusted by our internal partners and stakeholders, and, therefore, certain resources were transferred to us in an effort to achieve the objectives by developing adapted IT solutions. My biggest challenge has been to cope with this growth, complexity and sophistication while, at the same time, ensuring delivery of high-quality services, managing the risks and ensuring compliance. These challenges had to be met in a public-service context in which the constraints in terms of flexibility, value and legal compliance are very different from those in the private sector.

Feature

Every Silver Cloud Has a Dark Lining: A Primer on Cloud Computing, Regulatory and Data Security Risk

Carl Cadregari, CISA, is principal and practice lead in the Enterprise Risk Management Division of the Bonadio Group and also serves as chief information security director at one of the largest insurance companies in upstate New York (USA). Cadregari has more than 28 years of experience in IT and IS security architecture, deployment, project management, security by design and governance.

Alfonzo Cutaia, Esq., is an associate in the Information Technology & Internet Law Practice Group of Hodgson Russ LLP and focuses on patent practice. Before joining Hodgson Russ, Cutaia served as an intellectual property assistant for the Office of Science, Technology Transfer and Economic Outreach at the University at Buffalo (USA).

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.

In the ever-changing economic and regulatory climate, business needs can change as rapidly as the weather. Organizations need to be agile so that they can adapt to the storms on the horizon. Budgetary constraints and increased regulatory compliance initiatives have forced organizations to look at alternative solutions to their everyday needs.

One such alternative: cloud computing.

But, how does using the cloud impact business? How would an enterprise survive the loss of highly sensitive business and client information in the cloud and the potentially resulting fines, sanctions and lawsuits?

"Cloud computing" is a term that many have come across recently and that is sure to confuse. "Cloud" is a term borrowed by IT organizations from the telecommunication industry of the 1990s. It is more of a broad concept than an exact science. Cloud computing, in its broadest meaning and in theory, is the mass centralization of computing resources. Through this centralization, information, processing and software are made available to a multitude of companies, users and services by tapping into this normally remote, independently controlled cloud. Through the use of new technologies, including virtualization, new computer resources can be provisioned quickly by organizations that need additional resources.

Ironically, centralized computing was the original computing model—a centrally located mainframe computer provided processing power, while lower-power "dumb terminals" were connected to the mainframe from remote locations. Over time, as processing power became less expensive, the computing model moved to a client-server model, in which a local set of servers performed basic functions (e.g., file storage, print queue management), and the majority of computing power that existed at the edge of the network moved within laptops and desktop computers. Now, with the ubiquity of the Internet, the availability of previously unattainable data transfer speeds and the affordability of bandwidth, moving data and processing needs to relatively inexpensive and powerful computers at a cloud provider shows the return to a more centralized computing model.

Although cloud computing, as such, is still in its infancy, several cloud concepts have been in wide use. The business of data processing has grown accustomed to cloud computing terms and concepts such as application hosting, including Software as a Service (SaaS) and application service providers (ASP); storage virtualization, including cloud storage and online backup; IT outsourcing (ITO); and business process outsourcing (BPO), including help desks, virtual data centers and hosted (platform) data centers. However, despite this familiarity, the potential for harm from centralizing and sharing resources has grown to a level that can quickly exceed the business case for cloud computing. This risk must be understood by every organization contemplating the use of a cloud solution so that the organization succeeds, or even thrives, through its efforts.

THE SILVER CLOUD—MEASURABLE SAVINGS

The benefits of using cloud computing are numerous.[1] The shared nature and large scale of a cloud provider allow clients to quickly and easily scale their systems up or down to meet changing demands. This reduces the inefficiencies of traditional client-server deployments in which designers often overdesign capacity to ensure acceptable performance at peak demand. Also, many cloud-based systems enable users to access information from any web browser, even the latest smartphone and tablet platforms, and each user's consumption of resources can be monitored to maximize the efficiency of the system.

Enterprises that deploy cloud-based systems can avoid capital expenditures on hardware and capitalized software. Small enterprises may also benefit from the economies of scale of a cloud provider that is able to leverage

expensive resources—such as system administrators, backup infrastructure and network infrastructure—across multiple clients. All of these areas can ostensibly lower the barriers to entry because infrastructure is typically provided by a third party and does not need to be purchased for one-time or infrequent intensive computing tasks.

THE DARK LINING OF THE CLOUD

The benefits of cloud computing are tempered by the extreme potential to introduce uncontrolled or unforeseen risks and threats to an organization's information. Enterprises must fully assess, understand and mitigate all risks before moving data into the cloud.

The information needed to run a business is a valuable asset—sometimes tangible, sometimes not. What are its own data and information worth to an enterprise? How much would they be worth to a cybercriminal? What could a hacker do with the information? What would it cost the enterprise if another company accidentally accessed and changed the data? What would the enterprise do if it lost its information, or access to it, due to a disaster at the cloud provider? How would the enterprise know if someone changed the data? What is an enterprise mandated by law to do if its data were exposed?

Security vulnerabilities and data loss incidents are a regular occurrence. In 2010, according to *DataBreaches.net*, the US Federal Bureau of Investigation (FBI),[2] the Computer Security Institute (CSI)[3] and multiple other organizations that track these incidents,[4] there were hundreds of major incidents reported that encompass hundreds of millions of records—and those are just the reported ones. The reality is that one cannot open a newspaper or read an online article without realizing that cybercrimes and cybercriminals are a fact of life—just ask ALDI,[5] T.J.Maxx,[6] Heartland Payment Systems,[7] the US Veterans Administration,[8] Ben & Jerry's,[9] and PETCO,[10] to name a few. The bottom line is that using a cloud provider can significantly increase the risk of a security incident and can increase all the costs, legal remedies and other losses that follow such a breach. However, in addition to the increased risk of an event, the costs of determining what happened and recovering from the event may be compounded by the abstract nature of cloud computing itself.

Data, and access to them, have real value to the continued operations of an enterprise and especially to the clients it serves. At times, most assuredly, data are valuable enough for someone, some enterprise or even some country to want to steal, manipulate or otherwise compromise the information. How much the data are worth to a cybercriminal directly translates into an enterprise's threat posture. Attackers weigh their risks against their reward for getting that information. When using the cloud, the question becomes: What does centralizing data with the data of dozens or hundreds of other enterprises do to an enterprise's threat posture? The simple fact is that a business with data in the cloud has absolutely no direct control over where those data actually live. Also, standard service level agreements (SLAs) do not help much—cloud providers may do little, if anything, to ensure security, availability or response times for their clients. Most SLAs leave large time window carve-outs and best-effort hedges that do not provide concrete guarantees for business owners, especially as to their responsibilities under laws and regulations. Any time cloud computing is undertaken, data need to be reviewed, and at least the following six core questions from the Cloud Security Alliance[11] need to be answered and defined:

1. How would the enterprise be harmed if the asset became widely public and widely distributed?

2. How would the enterprise be harmed if an employee of the cloud provider accessed the asset?
3. How would the enterprise be harmed if the process or function were manipulated by an outsider?
4. How would the enterprise be harmed if the process or function failed to provide expected results?
5. How would the enterprise be harmed if the information/data were unexpectedly changed?
6. How would the enterprise be harmed if the asset were unavailable for a period of time?

REGULATORY COMPLIANCE IN THE CLOUD

To maintain compliance with the US Federal Information Security Management Act (FISMA); the US Health Insurance Portability and Accountability Act (HIPAA); the US Health Information Technology for Economic and Clinical Health (HITECH) Act; the US Gramm-Leach-Bliley Act (GLBA); the PCI Data Security Standard (PCI DSS); the US Family Educational Rights and Privacy Act (FERPA); the US Children's Internet Protection Act (CIPA); the US Sarbanes-Oxley Act; the 201 Code of Massachusetts Regulations (CMR) 17.00 (USA); California Senate Bill (SB) 1386 (USA); New York Information Security Breach Notification Act (NYISBNA) (USA); the US Code of Federal Regulations Title 21, part 11 (21CFR11); and other data security regulations, enterprises must have auditable requirements and actions. Therefore, enterprises need a thorough understanding of how using cloud computing affects their responsibilities and compliance actions. Generally, most laws and regulations require that an enterprise proves that its cloud provider (or ASP, SaaS provider and/or outsourcing host) has at least the same or similar controls in place as the enterprise's internally hosted systems to protect the data per the law or regulation affecting it. So, if an organization is a public company that relies on a cloud-based, third-party payment processor that also has collections responsibility and receives personally identifiable information (PII) from the organization, what does that cloud provider have to do? What does the enterprise have to do, and what happens when data are lost, inappropriately accessed or otherwise compromised?

COST OF A DATA BREACH

In today's world, misappropriated data, stolen and lost physical assets, and unintentional and intentional breaches occur with frightening regularity to every type and size of business. The recent study done by the Ponemon Institute regarding the cost and frequency of cybercrimes shows that the companies surveyed each had at least one successful cybercrime per week and that the annual cost of managing those attacks exceeds US $3.8 million.[12] The study details costs in most affected business areas, including cybercrime detection, avoidance, incident management and asset loss, but does not include noncompliance fines, sanctions and lawsuits that could easily double the true costs. Some recent fines levied include:

- **Rite Aid®**—US $1 million for a HIPAA violation[13]
- **The TJX Companies Inc. (of which T.J.Maxx is a part)**—US $40.9 million for lost credit card data[14]
- **Health Net of NE**—US $250,000 for a lost hard drive[15]
- **Six California (USA) hospitals**—More than US $790,000 by the California Department of Public Health (CDPH) for a privacy data breach[16]

As cloud computing grows, so will its exposure and use in criminal activity, as will the need for cloud forensics. This is evident in any recent data breach headline or on any data breach web site. For example, Cloutage.org (founded by the Open Security Foundation) stated that, in 2010, of the 322 incidents reported, 54 incidents of identified data loss occurred because the cloud provider was hacked or because a cloud vulnerability was found.[17]

ASSURING THE CLOUD

The use of cloud resources can be highly beneficial to most enterprises—but one should always know the risks, use the appropriate resources and experts from the audit and legal community, and be prepared to answer the following questions:

- **Security:**
  - How are data encrypted at rest and in transit?
  - How are data protected from unauthorized access?
  - How are data disposed?
  - How is cloud provider internal security handled?
    - Administrative controls
    - Physical controls
    - Logical controls
  - What rights and abilities does the enterprise have in the case of a breach (e.g., right to audit, ability to perform forensics investigations)?
  - What reporting obligations does the provider have to notify users of security breaches (e.g., indemnification for breaches)?

  - What actions has the provider taken to prevent attacks?
  - What protections does the provider require the enterprise to have in place?
  - How does the provider reliably demonstrate and communicate its security procedures to its clients?
  - How much ability does the provider give its consumers to perform their own assurance procedures, such as security scanning or audits?
  - How does the provider handle overlapping or contradictory interstate regulations on data privacy?
- **Compliance:**
  - What compliance standards does the provider meet?
  - How will compliance be maintained before, during and after a move to the cloud?
  - What third-party assurance (e.g., SAS 70, WebTrust, SysTrust, etc.) documentation is in place that assures compliance?
  - How can the enterprise track the physical location of its data for compliance (e.g., certain laws prevent data from being stored in certain countries)?
  - Beyond just data security, what documentation will be provided to the enterprise that will allow it to maintain compliance requirements with legislation such as the US Sarbanes-Oxley Act?
  - Is the enterprise prepared to maintain the needed internal controls and compliance to the levels required by all of its data?
  - At what point is too much information regarding internal controls and procedures being provided by the enterprise, thereby endangering the business?
- **Availability:**
  - How much uptime is guaranteed?
  - Is there a guaranteed service level? Who monitors it? What reimbursements will occur if the guaranteed level is not met?
  - Now that all services are accessed over the Internet, does the enterprise have enough bandwidth for all of its employees, and/or does the provider have enough power and bandwidth to service the enterprise's needs?
  - Can service be interrupted based on the activity of nonrelated cloud consumers (e.g., a hard drive subpoena)?
  - How is information segregated between clients?
  - How will assurance be provided by the cloud provider with regard to availability?
  - To what level is the cloud provider responsible, fiscally, legally or otherwise, for lost business as a result of service outages or issues?
  - What are the disaster recovery and business continuity plans once the enterprise has a cloud infrastructure?
- **Operations:**
  - How can the enterprise monitor the load and performance of the cloud?
  - How can the cloud provider assure the enterprise that it is being billed fairly for usage?
  - What tools are available and allowed to monitor security in the cloud?
- **Entire project:**
  - Who is the independent auditor for all the previously mentioned areas?
  - How often are the audits performed?

These questions are the most basic that should be answered when contemplating the use of a cloud provider; enterprises should be prepared to have in-depth technological, legal and business conversations on each. In all cases, an unsure or negative answer from the cloud computing vendor should be considered a deal breaker because even one poor control could be used to exploit all of an enterprise's data.

CONCLUSION

As cloud computing continues to push into the mainstream of information processing, data storage and cross-border communication, it is critical that the risks to data are consistently reviewed and that the threats identified are mitigated to a level commensurate with the value of the data. The value of a cloud computing infrastructure is measurable: savings can be achieved in data accessibility, customer relationship management, and decreased hardware costs and infrastructure support, but the costs of a breach or of lost data can easily outstrip any savings with the potential regulatory agency fines, civil lawsuits and reputational damage. Remember that it is always the enterprise's responsibility to keep its data confidential, maintain their integrity, assure their availability, meet its obligations under regulations and laws, and not get lost in the clouds.

ENDNOTES

[1] See the case studies published by Microsoft (*www.microsoft.com/en-us/cloud/tools-resources.aspx?CR_CC=200010704&WT.srch=1&WT.mc_id=A8A7CD18-DA39-4EEE-81FC-BA7440F28341&CR_SCC=200010704#casestudy*) and the information provided from VMware (*www.vmware.com/solutions/cloud-computing*).

[2] The Federal Bureau of Investigation, "Internet Crime Trends—The Latest Report," USA, *www.fbi.gov/news/stories/2011/february/internet_022411/internet_022411*.

[3] Computer Security Institute, *http://gocsi.com/sites/default/files/uploads/Surveyand%20webinar%20PR%202010.pdf*

[4] See *www.bankinfosecurity.com, www.ftc.gov, www.first.org, www.cloudsecurityalliance.org* and *www.cloutage.org*.

[5] ALDI, "ALDI Notifies Customers of Tampered Payment Card Terminals," press release, 1 October 2010, *www.aldifoods.com/us/media/company/company/Press_Release.pdf*

[6] Jewell, Mark; "TJX, Visa Reach $40.9M Settlement for Data Breach," *USA Today*, 30 November 2007, *www.usatoday.com/money/industries/retail/2007-11-30-tjx-visa-breach-settlement_N.htm*

[7] McGlasson, Linda; "Heartland Payment Systems, Forcht Bank Discover Data Breaches," *BankInfoSecurity.com*, 21 January 2009, *www.bankinfosecurity.com/articles.php?art_id=1168*

[8] Yen, Hope; "VA Agrees to Pay $20 Million to Veterans in 2006 Data Breach," *Boston.com*, 28 January 2009, *www.boston.com/news/nation/washington/articles/2009/01/28/va_agrees_to_pay_20_million_to_veterans_in_2006_data_breach*

[9] See Open Security Foundation, *http://datalossdb.org/incidents/3062-2-500-customers-names-and-addresses-exposed-on-the-web*.

[10] See Open Security Foundation, *http://datalossdb.org/incidents/30-up-to-500-000-credit-card-numbers-exposed*.

[11] Cloud Security Alliance, "Security Guidance for Critical Areas of Focus in Cloud Computing V2.1," USA, 2009, *www.cloudsecurityalliance.org/guidance/csaguide.v2.1.pdf*

[12] Ponemon, Dr. Larry; "Five Countries: Cost of Data Breach," Ponemon Institute LLC, revised 19 April 2010, *www.ponemon.org/local/upload/fckjail/generalcontent/18/file/2010%20Global%20CODB.pdf*

[13] Masters, Greg; "Rite Aid to Pay $1 Million Fine for HIPAA Violation," *SC Magazine*, 28 July 2010, *www.scmagazineus.com/rite-aid-to-pay-1-million-fine-for-hipaa-violation/article/175729*

[14] *Op cit*, Jewell, Mark

[15] Santalesa, Richard L.; "Health Net Agrees to $250,000 Fine and 'Corrective Action Plan' to Settle Loss of PHI," Information Law Group, 21 July 2010, *www.infolawgroup.com/2010/07/articles/hitech-1/health-net-agrees-to-250000-fine-and-corrective-action-plan-to-settle-loss-of-phi*

[16] Hennessy-Fiske, Molly; "Six California Hospitals Fined for Medical Record Security Breaches," *Los Angeles Times*, 19 November 2010, *http://latimesblogs.latimes.com/lanow/2010/11/hospital-fines.html*

[17] See Open Security Foundation, *http://cloutage.org/incidents?reported_year=2010*.

Questions That Must Be Addressed for a Successful IFRS Implementation

William C. Brown, CISA, CPA, is an assistant professor at Minnesota State University, Mankato, College of Business (USA). He has taught both accounting and management of information systems. His more than 25 years of experience include various levels of responsibility in positions including chief financial officer (CFO) in three US Securities and Exchange Commission (SEC) registrants. During his career, Brown has led several project teams to implement enterprise accounting and related systems.

Byron J. Pike, CPA, is an assistant professor at Minnesota State University, Mankato, College of Business. He has taught auditing and financial accounting at the undergraduate level. Pike has also worked as an auditor for a Big Four accounting firm.

The US Securities and Exchange Commission (SEC) is planning what could be among the largest changes in the history of American accounting—a conversion from Generally Accepted Accounting Principles (GAAP) to International Financial Reporting Standards (IFRS). This article integrates lessons learned from previous implementations of year 2000 (Y2K) enterprise resource planning (ERP) systems and the US Sarbanes-Oxley Act of 2002, and lessons learned from countries that have already adopted IFRS to provide an assessment that audit committees (ACs), chief financial officers (CFOs) and IT auditors can use to identify critical questions for a successful IFRS implementation.

CONVERSION TO IFRS

Approximately 29 million private businesses and 44,000 certified public accountant (CPA) firms in the US will be required to switch to IFRS-based standards.[1] The most likely effective date for an IFRS implementation will not come until 2016. A recent 2010 survey by Financial Executives International (FEI) and KPMG found that responders could attain an implementation deadline of 2016, if the IFRS decision is made in 2011.[2]

Canadian public companies must be IFRS-compliant starting in 2011. Of 146 senior executives responding to a 2010 Financial Executives Research Foundation (FERF) survey, most respondents from Canadian companies indicated that they were converting because their companies were publicly accountable—meaning, therefore, that conversion was mandatory. The survey also reported that the majority of companies were planning on running IFRS and Canadian GAAP in parallel.[3] Canadian IFRS implementation in small enterprises, which is similar to what is expected in the US, is often the responsibility of CFOs, who are also charged with most other financial management issues in their firms. Conversely, CFOs of large companies are more likely to be supported with adequate resources and staff devoted to the conversion. Dedicated IFRS teams for public companies in the Canadian IFRS implementation include accounting, IT, internal audit, treasury, risk management, human resources (HR) and investor relations.

For companies in the UK, Ireland and Italy that have already converted to IFRS, the biggest problem was the unexpected time commitment in understanding IFRS, in training, in assimilating requirements, and, for some, in major changes in IT.[4] The most difficult IFRS standards are those that require fair values, external data or key assumptions to be made to implement the standards. While most companies relied heavily on their auditors to advise them, complications arose when the Big Four audit firms did not agree on the treatment of certain items. The feedback from these countries suggests that the IFRS conversion should be viewed as a significant project.

While the timeline for the US adoption/convergence to IFRS is still unclear, there are several critical questions that corporate officers should be addressing now to achieve a successful IFRS implementation. These questions include:

- What are the requirements for IFRS?
- What has been learned from ERP and Sarbanes-Oxley implementation projects?
- What are the roles of COBIT and the Committee of Sponsoring Organizations of the Treadway Commission (COSO)?
- Do accounting and IT have the necessary project management (PM) skills?

Planning and appropriate resource allocations are necessary IFRS implementation requirements. Moreover, the implementation should be integrated with IT and internal controls in order to meet or exceed regulatory requirements.

IFRS REQUIREMENTS

The impact of IFRS on IT and financial systems can vary depending on the firm's IT and financial

systems' capability/integration, industry complexity, size, relevance of business process/transaction, internal control structure, mergers and acquisitions process, and other attributes.[5] Integrating both accounting and IT requirements for a multinational company exposes an array of variables that, in combination, can escalate the overall risk of an IFRS implementation.[6] Variables include:

- The intricacies of IFRS technical accounting standards
- An overlap of local and international regulatory considerations
- Conversion across business units and countries
- Separate IT systems within many organizations
- A limited number of IT professionals with IFRS technical knowledge who have the abilities to interpret and translate IFRS into IT changes

The effect of IFRS on IT varies from company to company, as evidenced by the results of a survey of Canadian public companies in which 61 percent said that the IFRS conversion would have a medium or high impact on IT systems, whereas only 27 percent of private companies expected a medium or high impact.[7] Some of the differences in perceived IFRS impact are attributable to the data collection and maintenance requirements.

Many authors describe the implementation of IFRS as a major system conversion.[8] Moreover, conversion to IFRS can be more pervasive to the enterprise than many perceive, will impact business operations and IT, and will require substantive system changes, modifications to business processes and new accounting policies.[9] The scope of the IT changes includes the entire food chain from data generation and business processes to final reporting (see **figure 1**).

While **figure 1** seems straightforward, United Technologies Corporation (UTC), an early adopter of IFRS, noted that a move to IFRS affects every aspect of business, with ramifications for everything from compensation to bonuses and budgeting.[10] The business model, including pricing, product costs and gross margins, is also affected. While **figure 1** identifies the data and applications affected by an IFRS implementation, the consequences must be understood in a business context, which involves a broad training effort inside the organization and corresponding lead times.

Figure 1—IFRS Requirements

IFRS Requirements	Type of Change
New data requirements	New data requirements may result in: • More detailed presentation of information • New data elements or fields to be recorded • Information to be calculated on a different basis
Changes to the chart of accounts	There will almost always be a change to the chart of accounts due to reclassifications and additional reporting criteria.
Reconfiguration of existing systems	Existing systems may already have capabilities built in to deal with the specific IFRS requirements.
Modifications to existing systems	New reports and calculations may be required to accommodate IFRS. Spreadsheets and models integral to the financial reporting process should be included when considering the required systems modifications.
Selection and implementation of new systems	Where previous financial reporting standards did not require the use of a system, or if the existing system is inadequate for IFRS reporting, it may be necessary to implement new software.
Interface and mapping changes	With the introduction of new source systems and the decommissioning of old systems, interfaces may need to be changed or developed, and changes to existing mapping tables to the financial system may be required.
Consolidation of entities	Under IFRS, there will potentially be changes to the number and type of entities that need to be included in the group consolidated financial statements.
Financial reporting tools	Reporting tools may need to be modified to: • Gather additional disclosure information from branches or subsidiaries operating on a standard general ledger package • Collect information from subsidiaries that use different financial accounting packages

Three international experts from companies in the midst of adopting IFRS warn against underestimating the IT challenges ahead, including the potential for millions of lines of new data for a large multinational organization.[11] One expert warned against using Excel spreadsheets as a solution to

handle the expanded IFRS data requirements. Assuming the IFRS requirements are met, traditional GAAP reporting must be maintained during the dual reporting period, which, ultimately, requires a complete reconciliation of GAAP and IFRS for each reporting period. For SEC registrants, US companies must report US GAAP and IFRS in parallel for three years from the initiation of IFRS. In creating a parallel accounting environment, the company's internal control and operational audit staff should evaluate prolonged modifications of IT support for dual reporting.[12] Internal control and operational audit staff can provide in-depth knowledge for conversion planning and ensure that overall conversion costs are comprehensive and accurate.

ERP IMPLEMENTATIONS AND SARBANES-OXLEY

A review of ERP implementations for Y2K, subsequent IT development and Sarbanes-Oxley provides a rich variety of lessons learned in IT governance and organizational maturity.

ERP

Deloitte Consulting[13] conducted in-depth interviews with 164 individuals at 62 Fortune 500 companies that used ERP systems, such as SAP, Baan, Oracle and PeopleSoft. The purpose of the study was to evaluate ERP development issues. The study summarized performance problems and the leading causes of such problems into three categories (see **figure 2**):

- **People**—62 percent
- **Process**—16 percent
- **Technical**—12 percent

Consistent with the reports from Deloitte Consulting, in the article "Managing Your ERP Project," Marie Benesh[14] described five areas of common management pitfalls that involve:

- Shortcomings in or a lack of integrated project team planning
- Managed communications across many people
- Formal decision-making processes
- Integrated test plans and managed test processes
- Failure to integrate lessons learned into current practices

In a survey of critical success factors (CSFs) throughout all stages of ERP implementations in 86 companies, factors similar to those reported by Benesh and Deloitte Consulting were ranked high in importance.[15] In-depth interviews with more than 50 chief information officers (CIOs) produced a similar theme: PM and process engineering skills were frequently mentioned as shortcomings in the course of enterprise development.[16] In their study of 541 large IT projects following Y2K, Weidong Xia and Gwanhoo Lee[17] demonstrated the influence of organization and personnel in large IT projects across several industries: Organizational aspects, including the use of qualified personnel, were the leading factors that contributed to project success.

Figure 2—ERP Barriers Focus

Barrier	Category
Lack of discipline	People
Lack of change management	People
Inadequate training	People
Poor reporting procedures: technical	People
Inadequate process engineering	People
Misplaced benefit ownership	People
Inadequate internal staff	People
Poor prioritization of resources	People
Poor software functionality	Technical
Inadequate ongoing support	People
Poor business performance	Process
Underperforming project team	People
Poor application management	Technical

Sarbanes-Oxley

The Public Company Accounting Oversight Board (PCAOB) assumed Sarbanes-Oxley regulatory oversight of approximately 15,000 companies and 1,423 accounting firms in the US.[18, 19] Three research reports on enterprises that reported at least one material weakness (MW) from 2002 to 2005 found that these enterprises were more likely to be smaller, younger, riskier, more complex and financially weaker, with poorer accrual earnings quality.[20, 21, 22]

Bonnie Klamm and Marcia Weidenmier Watson[23] examined 490 firms that reported MWs in the first year of Sarbanes-Oxley enforcement to evaluate the interrelatedness of weak COSO components and IT controls. Their research identified relationships between the reported MWs and the five components of COSO (control environment, risk assessment, control activities, information and communication, and monitoring), including:

- A weak control environment has a positive association with the remaining four weak COSO components, i.e., COSO components are likely to affect each other.

- Firms with weak COSO components related to IT frequently spill over to create more MWs and misstatements not related to IT.
- Weak COSO components related to IT negatively affect reporting reliability and add to the number of non-IT MWs reported.

Moreover, the conclusion from Klamm and Watson's research is that the IT domain appears to affect overall control effectiveness.

Cumulative evidence from Y2K ERP and subsequent IT project and Sarbanes-Oxley implementations suggest several risk drivers for IFRS:

- The scope of IT changes required to support IFRS
- The complexity of the enterprise, including the number of subsidiaries and the nature of assets and liabilities
- Smaller, younger, riskier, more complex and financially weaker organizations that lack either adequate resources or the leadership to execute change management

COSO/COBIT

The authors believe that the CSF lies in the organization's capability to execute an IFRS implementation while sustaining or improving internal controls as the accounting environment grows in complexity. A robust implementation of the COSO *Internal Control—Integrated Framework*,[24] an implementation of the COBIT[25] framework and a critical examination of the accounting organization for PM skills are effective responses to the risk drivers referenced earlier.

The COSO framework supports the establishment of an internal control framework for financial reporting, and COBIT supports the establishment of an IT framework for control and security. Together, they support the business process and information requirements, policies and standards necessary to support IFRS implementation and operation.

ACCOUNTING AND IT PM SKILLS AND THE CAPABILITY MATURITY MODEL

Accounting organizations that lack either adequate resources or the leadership to execute PM are among the most vulnerable in an IFRS implementation. Based on the previously mentioned research on Sarbanes-Oxley Act implementation experiences,[26, 27, 28] small to medium-sized enterprises (SMEs) represent the highest risk group for potential IFRS implementation issues. Moreover, many SMEs were never required to become compliant with Sarbanes-Oxley, and therefore, they lack the experience necessary for a complex implementation/conversion.

An assessment of the accounting organization is particularly meaningful because most accountants and CPAs are not trained for PM or systems implementations. If accountants have experience in any of these disciplines, it was more than likely obtained outside the roles of financial statement auditor or tax preparer, two major career paths that accountants often follow.

Young Hoon Kwak and C. William Ibbs[29] presented a PM model that progresses from an unsophisticated level to a sophisticated maturity level. Each maturity level consists of enhancements to major PM characteristics, factors and processes (see **figure 3**). Kwak[30] demonstrated that the average organization across several industries spends 6 percent of project value on total PM costs, which suggests an overall low cost given the potential range of adverse consequences for ineffective PM. In a study of 38 large international companies in four industries, overall PM maturity ranged from a low of 3.1 for information systems companies to a high of 3.4 for engineering construction companies, with an average for all companies of 3.3.[31]

In a scale with level 1 at the low end of maturity and level 5 at the high end of maturity, how should chief executive

Figure 3—Maturity Levels of Key PM Practices[32]

Level	Key PM Practices
Level 1, *Ad hoc*	• No PM processes or practices are consistently available. • No PM data are consistently collected or analyzed.
Level 2, Planned	• Informal PM processes are defined. • Informal PM problems are identified. • Informal PM data are collected.
Level 3, Managed at the project level	• Formal project planning and control systems are managed. • Formal PM data are managed.
Level 4, Managed at the corporate level	• Multiple PM program management exists. • PM data and processes are integrated. • PM processes data are quantitatively analyzed, measured and stored.
Level 5, Continuous learning	• PM processes are continuously improved. • PM processes are fully understood. • PM data are optimized and sustained.

officers (CEOs) or CFOs evaluate their organizational capability to initiate, plan, control and close out one-of-a-kind endeavors? At a minimum, any IFRS PM effort should not fall below the average benchmarks of 3.3 identified by Kwak and Ibbs.[33] At level 3, defined control systems are in place and adequately documented. The Capability Maturity Model (CMM) levels of 1 or 2 for a planned IFRS implementation *should not be acceptable* by an AC, the CEO or the CFO. With an emphasis on value and risk drivers, detailed analyses, tools and workshops, full support from business process owners, and accountability, a CMM level 3 for an IFRS implementation *may be acceptable*. COBIT integrates a CMM for internal controls, which is particularly important for a COSO/Sarbanes-Oxley-compliant organization (see **figure 4**).

Figure 4—Maturity Model for Internal Control (Extract)

Maturity Level	Status of the Internal Control Environment
Level 0, Nonexistent	• There is no recognition of the need for internal control. • Control is not part of the organization's culture or mission.
Level 1, Initial/*ad hoc*	• There is some recognition of the need for internal control. • The approach to risk and control equipment is *ad hoc*. • There is no communication or monitoring of risks or controls.
Level 2, Repeatable but intuitive	• Controls are in place, but are not documented. • Operation is dependent on the knowledge and motivation of individuals.
Level 3, Defined	• Controls are in place and adequately documented. • Operating effectiveness is evaluated on a periodic basis. • An average number of issues are outstanding.
Level 4, Managed and measurable	• A formal, documented evaluation of controls occurs frequently. • Many controls are automated and regularly reviewed. • Management is likely to detect most, but not all, control issues.
Level 5, Optimized	• An enterprisewide risk and control program provides continuous and effective resolution of control and risk issues. • Internal control and risk management are integrated with enterprise practices. • Internal control and risk management are supported with automated real-time monitoring with full accountability for control monitoring, risk management and compliance enforcement.

Source: IT Governance Institute (ITGI), COBIT 4.1, USA, 2007, p. 175

The authors believe that ACs and corporate officers should evaluate their internal organization skills as the project is fully defined and proposed. The evaluation should be based on the premise that:

1. Accountants and CPAs do not acquire PM skills in most available career paths.
2. Successful IT implementations are inextricably linked to qualified staff and effective PM.
3. SMEs are more at risk due to a lack of resources or effective leadership.
4. A minimum of CMM level 3 for internal controls should be attained for an IFRS implementation.

A priority for the AC, corporate officers and the IT auditor is to understand the IFRS impact on IT requirements because IT domain weaknesses spill over to other IT and non-IT internal control effectiveness areas in other COSO domains.

On a larger scale, for an IFRS conversion, the leadership of the SEC, the Financial Accounting Standards Board (FASB), the International Accounting Standards Board (IASB) and the American Institute of Certified Public Accountants (AICPA) should:

- Emphasize the organizational capability to implement and sustain an IFRS-compliant environment based on COSO/COBIT vs. a message that suggests a few courses in IFRS
- Develop well-defined requirements to drive a successful implementation and ongoing application of IFRS
- Create a conversion schedule that accommodates 29 million companies and the audit/consulting resources to support those conversions

CONCLUSION

For IT auditors and IT professionals, IFRS should be a priority because the demand will be high for those with technical knowledge to interpret and translate IFRS into IT requirements, COSO/COBIT-supporting references and audit programs. The capability to execute an IFRS implementation while sustaining or improving internal controls is a CSF. Lessons from Sarbanes-Oxley implementations indicate that IT and internal controls can be materially affected. The conversion to IFRS in the US will be a difficult and tenuous process for many companies. However, for those who learned from failed implementations in the past, IFRS will present an opportunity to move the organization to a higher CMM level of maturity while simultaneously adding capacity and flexibility for future endeavors.

ENDNOTES

[1] AICPA, "Looking to the Future: An Interview With AICPA President & CEO Barry Melancon, CPA," *CPA Letter Daily*, 15 December 2010, *www.smartbrief.com/servlet/wireless?issueid=FD77B3FB-FD54-4206-A7C6-C9E7E32E9BEE&sid=9a375f81-708d-44e5-a5f7-ca5c11478ab7*

[2] Goldschmid, Harvey; "IFRS at a Critical Crossroad," speech at the Financial Executives International (FEI) Current Financial Reporting Issues Conference 2010, held in New York, USA, 15–17 November 2010, *www.ifrs.org/News/Announcements+and+Speeches/IFRS+Critical+Crossroad.htm*

[3] Canadian Financial Executives Research Foundation (CFERF), "IFRS Readiness in Canada: 2010," Canada, 2010, *www.feicanada.org/pdfs/CFERF%20IFRS%20Readiness%20in%20Canada%202010.pdf*

[4] Institute of Chartered Accountants of Scotland, "The GAAP Gap," *CA Magazine*, 20 March 2008, *www.camagonline.co.uk/Magazine/2008-3/64.aspx*

[5] American Institute of Certified Public Accountants (AICPA), "Financial System Considerations in IFRS Conversion Projects," USA, 2010, *www.ifrs.com/pdf/10414-378_IFRS_IT_White_Paper_WEB_FINAL.pdf*

[6] KPMG LLC, "Information Technology Advisory Services: The Effects of IFRS on Information Systems," USA, 2008, *https://www.in.kpmg.com/securedata/ifrs_Institute/Files/Effects_of_IFRS_on_IS.pdf*

[7] *Op cit*, CFERF

[8] Difazio, Nick; D.J. Gannon; "IFRS Roadmap: Planning a Safe, Economical Trip," *Deloitte Review*, 20 January 2010, *www.deloitte.com/view/en_US/us/Insights/Browse-by-Content-Type/deloitte-review/article/3391e6545eea2210VgnVCM200000bb42f00aRCRD.htm*

[9] Arnold, Steve; "IFRS Risk Planning and Controls Execution: Strategic Considerations for Financial Managers," *Journal of Accountancy*, September 2009, *www.journalofaccountancy.com/Issues/2009/Sep/20091594*

[10] AICPA, "Getting to IFRS: Those Who Have Been There Have Plenty of Advice," USA, 2009, *www.ifrs.com/advice.html*

[11] *Ibid*.

[12] *Op cit*, Arnold

[13] Deloitte Consulting, *ERP's Second Wave: Maximizing the Value of ERP Enables Processes*, 1999, *www.ctiforum.com/technology/CRM/wp01/download/erp2w.pdf*

[14] Benesh, Marie; "Managing Your ERP Project," *Software Testing and Quality Engineering*, July/August 1999, p. 38–43

[15] Somers, Toni M.; Klara Nelson; "The Impact of Critical Success Factors Across the Stages of Enterprise Resource Planning Implementations," Proceedings of the 34th Hawaii International Conference on System Sciences, IEEE, USA, 2001

[16] Reich, Blaize Horner; Kay M. Nelson; "In Their Own Words: CIO Visions About the Future of In-house IT Organizations," Database for Advances in Information Systems, 1 October 2003, *www.allbusiness.com/technology/3502741-1.html*

[17] Xia, Weidong; Gwanhoo Lee; "Grasping the Complexity of IS Development," *Communications of the ACM*, 1 May 2004, *http://cacm.acm.org/magazines/2004/5/6513-grasping-the-complexity-of-is-development-projects/abstract*

[18] McDonough, William J.; "The PCAOB and Its Oversight Role," Public Company Accounting Oversight Board (PCAOB), speech at the Joint Financial Management Improvement Program in Washington, DC, USA, 9 March 2004, *http://pcaobus.org/News/Speech/Pages/03092004_McDonoughJointFinancialManagement.aspx*

[19] PCAOB, "Board Approves Revised 2005 Budget," USA, 30 December 2004, *http://pcaobus.org/News/Releases/Pages/12302004_Revised2005Budget.aspx*

[20] Doyle, Jeffrey; Weili Ge; Sarah McVay; "Determinants of Weaknesses in Internal Control Over Financial Reporting," *Journal of Accounting and Economics*, September 2007, *http://home.business.utah.edu/sarah.mcvay/DGM_2007_JAE.pdf*

[21] Doyle, Jeffrey; Weili Ge; Sarah McVay; "Accruals Quality and Internal Control Over Financial Reporting," *The Accounting Review*, vol. 82, issue 5, 2007

[22] Ge, Weili; Sarah McVay; "The Disclosure of Material Weaknesses in Internal Control After the Sarbanes-Oxley Act," *Accounting Horizons*, September 2005, *www.uic.edu/classes/actg/actg593/Readings/Stock-Options/Sarbanes-Oxley/The-Disclosure-of-Material-Weaknesses-in-Internal-Control-after-the-Sarbanes-Oxley.pdf*

[23] Klamm, Bonnie; Marcia Weidenmier Watson; "SOX 404 Reported Internal Control Weaknesses: A Test of COSO Framework Components and Information Technology," *Journal of Information Systems*, Fall 2009

[24] Committee of Sponsoring Organizations of the Treadway Commission (COSO), *Internal Control—Integrated Framework*, USA, 2004

[25] IT Governance Institute (ITGI), COBIT 4.1, USA, 2007, *www.isaca.org/Knowledge-Center/cobit/Pages/Downloads.aspx*

[26] *Op cit*, Doyle, Jeffrey; Weili Ge; Sarah McVay; "Determinants of Weaknesses in Internal Control Over Financial Reporting"

[27] *Op cit*, Doyle, Jeffrey; Weili Ge; Sarah McVay; "Accruals Quality and Internal Control Over Financial Reporting"

[28] *Op cit*, Ge, Weili; Sarah McVay; "The Disclosure of Material Weaknesses in Internal Control After the Sarbanes-Oxley Act"

[29] Kwak, Young Hoon; C. William Ibbs; "Project Management Process Maturity (PM)² Model," *Journal of Management Engineering*, July 2002, *http://home.gwu.edu/~kwak/PMPM_Model.pdf*

[30] Kwak, Young Hoon; "A Systematic Approach to Evaluate Quantitative Impacts of Project Management (PM)," doctoral dissertation, Department of Civil Engineering, University of California, Berkeley, USA, 1997

[31] Kwak, Young Hoon; C. William Ibbs; "Calculating Project Management's Return on Investment," *Project Management Journal*, June 2000, *www.lamarheller.com/projectmgmt/calculatingpmroi.pdf*

[32] *Op cit*, Kwak, Young Hoon; C. William Ibbs; "Project Management Process Maturity (PM)² Model"

[33] *Op cit*, Kwak, Young Hoon; C. William Ibbs; "Calculating Project Management's Return on Investment"

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.*

Automated Audit Testing for SAP Data—Benefit or Just Another Black Box?

Stefan Wenig is chief executive officer (CEO) of the dab:Group, a company that specializes in data extraction, analysis of SAP data with ACL and automated audit routines. He has participated in developing data extraction software and is a consultant and globally active trainer for data analysis techniques. Wenig has been supporting internal audit departments in the field of data analysis for years.

Kyung-Hee Anita Kim-Reinartz is branch manager of the Dusseldorf (Germany) office of the dab:Group. Prior to joining the dab:Group, she worked for PricewaterhouseCoopers for more than nine years. Kim-Reinartz's specialties are forensic data analysis and, notably, continuous controls monitoring. She was a project manager of the worldwide continuous controls monitoring implementation of a large German technology company.

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.

Automated audit testing has been discussed for many years. Buzzwords such as "continuous auditing" and "continuous monitoring" arose and have been talked and theorized about. In particular, internal auditors and public accountants who have to cope with increasing requirements in testing and compliance regulation are searching for more intelligent and integrated methods of automating testing. However, while evaluating IT tools and ways of standardizing audit routines, questions may arise regarding whether automation is really the future or whether there is the risk of creating a "black box": a tool that makes auditors lose certainty and trust in the results due to the uncertainty about how the results were generated. False positives—results that turn out not to be real findings—may even support this reluctance.

This article discusses ways to standardize data extraction and audit routines. It is written based on SAP data, but this is exemplary for all complex enterprise resource planning (ERP) systems. Furthermore, the article discusses how to handle increasing amounts of data and how to avoid creating a black box.

OVERVIEW OF THE ISSUE

The methods of digital data analysis are getting more and more important in the globalized world. The reasons are obvious:

- External requirements such as legal or compliance aspects require more transparency (100 percent of transactions), preferably in real time (immediately).
- Business processes are implemented on highly integrated and complex ERP systems such as SAP.
- Globalization and technological progress lead to the generation of mass data in day-to-day business. Having to deal with large data sets and a growing variety of audit questions makes time the most essential resource for auditors.
- Data extraction and data analyzing tools are getting more powerful.

Large companies or conglomerates usually have ERP systems, such as SAP or Oracle Financials, in place—at least for their most important legal entities that cover the essential part of the transaction volume. However, instead of hosting a clutter of systems, most companies tend to harmonize their IT landscape and move toward a more standardized and integrated system. It is important to note that the databases of ERP systems are standardized up to a point. This means that the core table and field names of the data, which are necessary for standardized automation, are the same worldwide. Hence, audit routines can be predefined and are then generally applicable—worldwide, cross company and, at least within the core processes, independently of the business areas of an enterprise. Therefore, the vendor master data within nearly any release version of the SAP system can always be found in the vendor master-general section table—independent of any parameters such as company, system and location, as long as it is a standard SAP system. However, for other data that cannot be located that easily, a profound understanding of the data and the underlying business processes is inevitable.

Furthermore, not only auditors, but various departments are facing more and more internal and external requirements that occur due to compliance issues, legal aspects and tax regulations, for example. Abnormal transactions have to be detected and reported immediately; legal aspects and tax regulations require reporting to be published/reported in faster cycles. This shows that time and mature technology are crucial factors to enable enterprises to meet these requirements.

In a globalized and computerized world, particularly well-established business processes such as purchase-to-payment (P2P) and order-to-cash (O2C) are creating more and more data every day.

Analyzing that mass of data requires more powerful audit tools. Server solutions and continuous controls monitoring (CCM) tools were developed to meet these increasing requirements. For years, it has been shown that using audit software for substantive testing to provide total assurance or clear pinpointing of errors and fraud greatly increases the credibility and value provided by the audit function.[1] However, despite the fact that the software is getting more powerful and keeps up with the business situation, internal audit is challenged by this development. In a situation in which, in theory, 100 percent of all relevant transactions can be tested and a catalog full of audit questions is to be run against the data, time is of essential importance. Additionally, legal and compliance requirements are creating the need for enterprises to be aware of all information these huge quantities of data may contain.

OVERVIEW OF THE SOLUTION

How does an enterprise cope with these challenges to facilitate and automate all required testing of 100 percent of a data population and meet the expectations of stakeholders regarding automated testing? Implementing an effective solution that will meet the demands needs to consider multiple issues including how to:

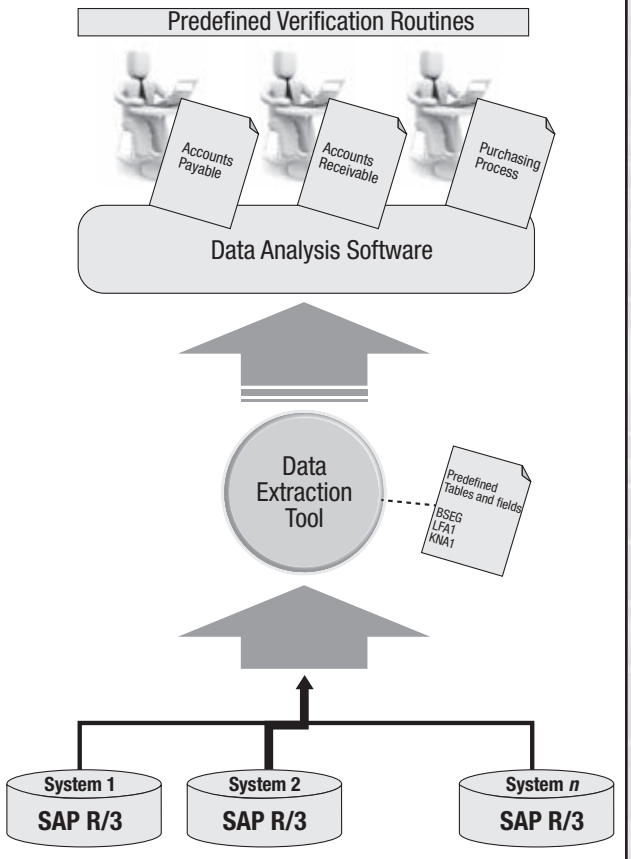
- Access the right data
- Analyze mass data without compromising the performance of productive systems
- Analyze data effectively and with a minimum number of false positives
- Avoid creating a black box

Basically, the solution consists of two main parts (see **figure 1**):

1. Extract the raw data from the database.
2. Analyze them on a separate machine with special auditing software by running predefined verification routines to cover the basic audit questions.

These two main aspects are explained in detail in the following subsections. The SAP system (or systems—larger enterprises usually have more than one) is visualized at the bottom of **figure 1**.

Figure 1—Solution Overview for Appropriate Data Extraction



Source: dab:Group, Germany, 2001

The relevant data that are in the SAP database need to be extracted from the system by a special data extraction tool. There are various data extraction tools available—the most

important points to consider will be discussed in the following section. The document depicted in **figure 1** represents a list of tables and fields that are necessary for a certain audit, so only the important data are extracted. Ideally, the extraction tool facilitates conversion of the extracted data into a format readable by the data analysis software used on the data. Therefore, no additional formatting or time-consuming import procedure has to be performed. Usually, there are several predefined tests implemented within the data analysis software that can be immediately performed on the data. They are standardized and cover the most important audit questions. Typical examples include searches for vendor master data duplicates, invoices not based on a purchase order (PO) and manual payments; analysis of one-time accounts; general ledger (GL) testing; and cash recovery aspects such as double-payments analysis.

Data Extraction

The approach to have data extracted from the system is subject to the assurance of the business continuity of the ERP system. If large and complex tests of the entire population of data were run directly on the SAP system (using reports, etc.), it would have considerable impact on system performance, which would impede business operations. When reports take too long to complete, they time out. Hence, having the data extracted to a separate machine, which can be a server or even just an auditor's laptop, is usually the better option. Instead of taking the risk of the issues mentioned, the separate computer can do the heavy-duty part of the analysis without impacting the performance of the SAP system. The count and complexity of the tests executed do not matter. For example, executing five database-intense reports on the SAP system would impact system performance five times. Downloading the data once and running 50 standardized, predefined audit routines will impact the system once during the download. Hence, "download once, analyze often" is the best practice in this situation. There are a few more things to consider when extracting data:

> "'Download once, analyze often' is the best practice."

- **Transparency**—Most data extraction solutions need to have components installed on the SAP server. It is important that, whatever needs to be implemented, there is no complexity and the instructions for implementation are clear and concise. The layout should be transparent enough to keep IT effort to a minimum. There should be minimal need for testing and evaluation of additional components in the system because the potential impact of data extraction on the ERP system needs to be carefully considered.
- **Read-only access**—On the client side, any user who needs access to the data must have the authorization only to read data. This is important because, during data extraction, data in the system must not be accidentally changed.
- **Reliability**—The reliability of the source and content of information is crucial—not only in traditional auditing, but also in computer-aided auditing techniques.[2] The reliability of the data is one of the most crucial aspects in data analysis. If the enterprise cannot rely on the extracted data, every subsequent step is useless. Without assurance regarding completeness, validity and accuracy, every interpretation of data is guesswork at best. For example, there are data extracted from a GL that originally contained 100 data sets, but only 96 data sets have been extracted. If the data are profiled, the range of entries is between 100,000 and 500,000, but one of the four missing data sets may indicate an entry with an amount of 800,000. This would make every query based on this information worthless, particularly with regard to materiality aspects. An audit issue regarding an amount of 200,000 would make up 40 percent in the first case and 25 percent in the second. Therefore, one of the important aspects when considering a data extraction tool is to have documentation of the data extraction process to be able to check for completeness, validity and accuracy later.
- **Independency and usability**—Data access is an important element for audits. If there is a delay of several weeks before data are delivered, a time problem may result that impacts the audit plan. The risk of receiving (accidentally or intentionally) manipulated data is another issue. Both of these points can be solved by equipping auditors (or a special team within the internal audit department) with data extraction tools for extracting the data on their own while considering the necessity of the adjustment in the system for read-only access. Easy-to-use tools with a graphical user interface (GUI) that allow a user-friendly practice, even for financial or operative auditors, are key to growing acceptance for data extraction solutions.

- **Mass data capability**—As outlined previously, the database in the SAP system can contain huge amounts of data. For audit purposes, the GL tables accounting document header and accounting document segment or the change log tables change document header/change document items, where millions of changes are recorded, are very important. The tables accounting document header and accounting document segment contain all the financial documents, and the change log tables record a variety of events such as the removal of payment blocks, vendor master data changes, credit limit updates and price changes in sales documents. For conglomerates, it is not unusual for these tables to reach a count of almost one billion records, resulting in file sizes of several hundred gigabytes of data. The extraction tool must be able to cope with these volumes of data without causing timeouts or overly impacting the SAP system.

> "Defining and identifying the appropriate subject matter are crucial for both automating the process and reading the results."

Data Analysis With Analyzing Tools and Predefined Tests

Designated data analysis software usually allows programming/scripting and coding to create user-defined tests. The scripting language, in combination with the globally standardized table and field names of an SAP installation, allows for standardizing audit tests. This means that once the data have been extracted, these tests can be performed automatically and without manual effort.

The essentials of data analysis and testing include:

1. Interesting subject matters for auditing—how to gather audit evidence
2. The benefits of using predefined audit routines
3. The challenges that an audit department could face when running standard tests

Interesting Subject Matters

Since the most important business processes are usually mapped to the SAP system, a variety of audit subject matters can be analyzed. Defining and identifying the appropriate subject matter are crucial for both automating the process and reading the results. Subject matters that are fairly definable and measurable facilitate automated audit testing. Audit questions depend on the focus of each audit, but also on the audit department in general. Some standard tests, grouped by topic, include:

- **Cash recovery aspects**—Double payments, discount losses, open items analyses
- **Fraud analyses**—Payments to vendors or banks located in a tax haven, payments to alternate payees, pattern analysis of business partners, bank account changes
- **Master data tests**—Customer or data duplicates, missing tax IDs, incorrect master data
- **Checks for identifying process weaknesses**—Manual payments or invoices not based on POs

Benefits

A standardized approach can have valuable benefits. In every audit, the basic questions can be answered almost at the push of a button, providing a lot of advantages, such as:

- Standardized, reliable algorithms based on years of auditor experience
- Auditor experience transferred to technical know-how
- Documented know-how in a structured form
- Opportunity to generate key performance indicators (KPIs)
- Support for creating the audit plan, obtaining transparency about audit items
- Obtaining reliable results quickly

The audit routines always use the same algorithm, so the results are comparable. On the other hand, when doing the testing manually, two auditors may be doing the same test correctly, but in a slightly different manner (e.g., one may include intercompany transactions while the other does not), so the results are not comparable. With standardized testing routines, they always are. The audit routines can also provide a basic set of KPIs that immediately give an overview of a certain topic—for example, all company codes. Therefore, the KPIs that are generated can be used for creating the audit plan, assigning the resources to audits of business units in which the risk may be higher than in others according to the indicators. Even audits that require travelling can now be prepared beforehand. Traditionally, auditors travel, sometimes to another country, to visit the legal entity; request the data from the IS department onsite; wait for the data; and import them manually into the auditing software. It can often be one or two weeks before the auditors are finally able to have a detailed look at the situation. Things can now be sped up considerably. The data can be downloaded in advance, the

planned audit steps can be performed and the results can be examined before even leaving corporate headquarters. This allows for in-depth interview preparation.

Challenges

Using predefined audit tests in combination with a data extraction tool offers a lot of advantages. As with any new approach, using predefined tests can also bring challenges, such as:

- Technical issues related to the data extraction tool
- False positives within the predefined audit routines
- User acceptance

Technical challenges exist, but they are usually not insurmountable. The data extraction software has to be installed on the SAP system and on the auditor's laptop or other client systems. Regarding the server components, the software has to go through the whole cycle of test systems and quality assurance systems before it can be used on the productive system. Moreover, the user profiles have to be adjusted for the users that are designated to perform the data extraction.

In the analysis of the data by the predefined audit routines, false positives are usually an issue. There is one simple rule: The more exact the company's policies and guidelines are, the fewer false positives are expected. For example, if the guideline for master data states only that the telephone numbers have to contain country codes, then the numbers 0049 999 111 22, +49 (0) 999 111-22 and +49 (999) 11122 will all be correct, but hard to test in a standardized way. If the format has to be +CC (PREDIAL) NUMBERWITHOUTBLANKS, only the third option is correct, and a test will be easy to implement with a restrictive algorithm that is unlikely to create a lot of false positives. Other examples include the analysis of invoices without POs. There are companies in which 100 percent of the nonintercompany invoices have to be based on POs. This is easy to test: Any nonintercompany invoice not referring to a PO is a violation. However, if there are 25 exceptions in the definition, it becomes a lot more difficult to test.

The huge number of results due to false positives is one of the challenges for growing user acceptance. However, most auditors without an IT background have a great degree of difficulty in integrating data analytic skills with their professional knowledge in auditing. This limitation greatly impairs the auditor's ability to independently and continuously perform and understand data analytic semantics—and, even more, the results.[3] In the future, auditors must develop a mix of capabilities, competencies and experience levels, with one of the most essential capabilities being the ability to conduct data analysis.[4] Proper training and the perspective of the work becoming easier in the long run—leaving more time for testing new audit methods for shifting from a traditional internal audit to a risk-centric model—can help auditors alter their mindset to meet the requirements of the future.[5] If the IT auditors are assigned to the automation of the process and the finance auditors are designated to just use the results, an appropriate interaction and communication between both teams is necessary for avoiding the black box effect.

> "The more exact the company's policies and guidelines are, the fewer false positives are expected."

CONCLUSION

In automated auditing projects for companies and audit departments of any size, the following elements are key to success:

- Extracting the raw data
- Avoiding a black box by well-defined analysis, appropriate training and good communication
- Maintaining flexibility and avoiding a purely check-list audit
- Considering server-supporting analyzing solutions because they may be the future for mass data

Without a proper data extraction tool, setting up standardized and well-defined audit routines is almost impossible. Data of any size must be extracted from the systems, and they must always be in the same format so that audit routines can be based on these data structures.

For the audit department and the auditors, as users of the solutions, digital data analysis has to be a time-saving solution and a solution that creates results that the auditors trust. Clear, to-the-point documentation of the audit steps, in combination with training on each important topic (SAP tables and fields, business process aspects, software tools), is extremely important to avoid the black box

effect. Continuously integrating experiences into the process also helps to fine-tune the analysis and, therefore, may decrease the number of results. Having a team of people with a mixed and balanced distribution of business process and IT backgrounds also facilitates avoiding black box effects.

Moreover, the predefined routines and the results are elementary for the auditors' fieldwork. Their flexibility to bring their own creativity is crucial. Digital data analysis is not intended to be a fully automated report generator; it is a way to fully automate the preparation of the base for their actual work in a reliable, fast and transparent way.

The quantity of data nowadays is huge. Unquestionably, it will increase more and more through the years. Digital data analysis and dealing with data in a structured, logic and effective way is the future. The sooner the first steps are made, the more future-proof the profession of internal audit will become.

ENDNOTES

[1] Sayana, S. Anantha; "Using CAATs to Support IS Audit," *Information Systems Control Journal*, vol. 1, 2003

[2] See the International Accounting Standards Board (IASB) International Accounting Standard (IAS) 330 and ISACA's IT Audit and Assurance Standards, Guidelines, and Tools and Techniques, *www.isaca.org/standards*.

[3] Li, Shing-Han; Shi-Ming Huang; Yuah-Chiao G.Lin; "Developing a Continuous Auditing Assistance System Based on Information Process Models," *Journal of Computer Information Systems*, fall 2007

[4] PricewaterhouseCoopers LLP, "Internal Audit 2012: A Study Examining the Future of Internal Auditing and the Potential Decline of a Controls-centric Approach," USA, 2007

[5] *Ibid*.

The Assimilation of Marketing's Service Quality Principles and the IT Auditing Process

A Move Toward Quantifiable SAS 70 Auditing Service Quality, Part 1

Thomas J. Bell III, Ph.D., CISA, PMP, is a professor of business administration in the School of Business at Texas Wesleyan University in Fort Worth, Texas, USA, and an IT security auditor for ComputerMinds.com in Euless, Texas, USA. His IT auditing specialty is IT audits for small community banks (IT security audits and external penetration testing) and SAS 70 Type I and II audits.

Thomas Smith, Ph.D., is a professor of marketing and mass communication in the School of Business at Texas Wesleyan University in Fort Worth, Texas, USA. His publications include articles about advertising theories and practices in addition to creative marketing. He also has decades of service marketing experience.

Certainly, service quality should not be taken for granted, yet it is a topic that is seldom mentioned in association with IT auditing services as performed by an IT auditor. Most of the literature seems to address the methods, tools and techniques of auditing, with scant attention devoted to the actual quality of the IT auditing services being rendered. The need for businesses to pay attention to the quality of services being delivered to customers has grown over the past decades as the economy has journeyed from a secondary-sector economy into a large and growing tertiary-sector economy.

The tertiary sector of the economy (commonly referred to as the service sector/service industry) is one of three economic sectors, the other two are the secondary sector (manufacturing) and the primary sector (agriculture). The tertiary sector's basic attribute is the production of services as a replacement for some finished products, which may include activities in which people offer their services, knowledge and time to improve productivity and performance. Such tertiary-sector services include IT auditing and consultancy services.

This article, which is the first part of a two-part series, discusses techniques that IT auditors can use to improve the quality of their Statement on Auditing Standards (SAS) No. 70 auditing services. The second part (look for it in volume 4, 2011) of this article describes the development of a multiple-item scale for measuring service quality and how service quality properties can be assimilated into SAS 70 auditing services.

An organization seeking a SAS 70 Type I or Type II compliance audit is certainly interested in the costs of these audits, including all the hidden fees, given the vast differences in SAS 70 pricing (and quality) of work from one firm to another. At issue is how to conduct a SAS 70 audit that meets the client's needs while also providing quality service and techniques to assess quality auditing services. Meeting the needs of the customer will be examined through the lens of understanding customer perceptions and the customer's role in SAS 70 auditing services by assimilating marketing's time-tested service quality framework, SERVQUAL, into the IT auditing process.

SAS 70 AUDIT OVERVIEW

SAS 70, Service Organizations, is an auditing statement developed by the Auditing Standards Board of the American Institute of Certified Public Accountants (AICPA) with its content codified as Accounting Unit (AU) section 324. A SAS 70 audit is broadly recognized because it provides reasonable assurance that a service organization has been through an in-depth audit of its control activities, which generally includes controls over IT and related processes.

In cases in which data are regulated and/or sensitive, it is important for hosting service organizations to have detailed and well-documented controls in place to ensure the safety and privacy of the data being processed, stored and transmitted. Perhaps most notably, the requirements in section 404 of the US Sarbanes-Oxley Act of 2002 heighten the importance of SAS 70 audit reporting on the effectiveness of internal control over financial reporting. A SAS 70 audit serves as an indicator of transparency and accountability; it establishes a high level of commitment by the service organization toward ensuring the reliability and security of its data by having its internal controls and activities examined (via an in-depth audit of control, which often includes controls over IT and related processes) by an independent auditing firm.

Enjoying this article?

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

www.isaca.org/whitepapers

- Learn more and collaborate on SAS 70 in the ISAE 3402 topic.

www.isaca.org/knowledgecenter

SAS 70 provides guidance to service auditors for assessing the internal controls of a service organization and issuing a service auditor's report. SAS 70 also provides guidance to auditors of financial statements of an entity that uses one or more service organizations. Service organizations are typically entities that provide outsourcing services that impact the control environment of their customers or user organization.

A formal report, called a service auditor's report, which includes the auditor's opinion or attestation statement, is issued to the service organization at the conclusion of a SAS 70 audit. This report is effectively an auditor-to-auditor communiqué between the service and user organization (the entity that has engaged a service organization, particularly if its financial statements are impacted by the services of the service organization). There are two different, yet complementary, types of SAS 70 audit reports: Type I and Type II.

SAS 70 Audit—Type I

Type I includes an opinion of the fairness of the presentation of the service organization's description of controls that have been placed in operation and the suitability of the design of the controls to achieve the specified objectives. Type I reports describe the degree to which the service organization fairly represents its services in regard to controls that have been implemented in operations and its inherent design to achieve objectives set forth. The depth of this audit is limited because it states the presentation and design of controls in place in terms of their ability to meet defined control objectives, but does not test their effectiveness. This report typically examines controls over one or two days only, which, arguably, has limited value to a user organization.

SAS 70 Audit—Type II

A Type II service auditor's report is the most thorough report of a SAS 70 audit because it contains a description of the controls in place and also includes a description of the auditor's tests of control effectiveness for a minimum testing period (usually the defined period is six months, but it can be longer). The Type II examination of the SAS 70 audit process begins similarly to Type I, but includes additional testing and observing procedures. Such procedures analyze and test the controls *vis-a-vis* Type I, but also include the service auditor's opinion on how effectively the controls operated under the defined period during review. The Type II service auditor's report will state "whether the controls that were tested were operating with sufficient effectiveness to provide reasonable, but not absolute, assurance that the control objectives were achieved during the period specified."[1]

A Type II service auditor's report is more common and often the preferred choice of SAS 70 audits because it is a comprehensive analysis of not only what controls are in place, but also of how effective those controls are in meeting the desired objectives.

SAS 70 AUDIT PROCESSES

Service consists of several processes or performances, and to accurately understand SAS 70 auditing quality, a requisite examination of the auditing process is essential. A SAS 70 audit is a structured, multistep process that includes a number of predefined processes that are grouped into five categories called process groups: initiating, planning, executing, monitoring and controlling, and closing.[2] These process groups provide guidance and procedures necessary to ensure successful and orderly audit completion. These process groups, which are summarized in **figure 1**, offer some general process guidance for audit projects.

Depending on a service organization's needs, a SAS 70 Type II audit is generally performed for a specified period following the completion of a Type I audit. Successfully completing a SAS 70 Type I audit and then moving in the direction of a more comprehensive Type II audit has been the traditional path many service organizations have taken.

Figure 1—SAS 70 Process Groups	
Process Group	**Process Description**
Initiating	First phase of a SAS 70 audit project. It may include basic audit definition/understanding, authorization and assurance that the project fits with the business needs before more in-depth planning begins.
Planning	May include defining objectives, requirements, staffing, budget, dependencies and scope, and also determining how to attain the scheduled objectives and how to budget resources and the team. The audit manager must also build in a good communication plan for the project team and stakeholders.
Executing	Involves coordinating the audit team's efforts, resources and communication to carry out the plan while keeping constant contact with the team's stakeholders. Ensuring quality assurance is an essential element of the execution process, requiring constant monitoring to ensure that the audit meets the specified requirements.
Monitoring and controlling	Involves monitoring project progress at regular intervals to ensure that the project stays on course as planned—particularly in terms of scope, schedule and cost
Closing	Includes obtaining formal acceptance of project completion from the client, closing the project and reviewing the lessons learned

The need for a Type II audit may depend on a variety of reasons, but primarily it is driven by publicly traded companies having to certify their internal controls that have been outsourced to a service organization that provides a significant function. This audit is required under section 404 of the US Sarbanes-Oxley Act, and as a result, a Type II audit is necessary for many service organizations.

SAS 70 Type I and Type II audits can be improved by using quality management principles that may involve a variety of self-assessment and measuring tools. Such tools may examine quality issues as they relate to fitness for purpose and conformance to standards while others relate to quality costs or the lack thereof.

MEASURING SAS 70 AUDIT QUALITY

According to the marketing literature, service quality and satisfaction are related items.[3] "Satisfaction" is defined as the emotional evaluation of a perceived discrepancy between expectations and performance of a product or service.[4] Correlating in-process improvement with customer perceptions has traditionally been difficult. Success in solving this problem could lead to ways of predicting customer satisfaction with likely process improvements to follow. Changing the IT auditing process in the expectation that quality, as observed by the customer, will improve is the challenge.

The goal is to find a satisfactory way to quantify customer perception of IT auditing quality to assess how process improvements can lead to better user experiences. The focus is to find a practical approach to measure customer perception of IT auditing quality, implement it in an organization and validate its performance through some metric.

Measuring the quality of a service can be a convoluted charge. Unlike products, for which there are specific physical specifications such as height, width, weight and color, a service can have numerous intangible or qualitative specifications. Service considerations may include customer service expectation, which can vary considerably based on factors such as personal needs, prior experience and what other people may have said about their IT auditing experiences.

Quality problems are often examined through an understanding of customer service satisfaction because service quality is closely related to customer satisfaction, customer retention and positive word of mouth.[5] According to research,[6] the best way to understand service effectiveness is through customer perceptions. Customer perceptions are critical in any product context, and in the world of service delivery, customer perception is perhaps even more important given the personal and interactive nature of services. It is quite possible to satisfy every written or stated requirement and still fall short of satisfying the customer. The guidelines sometimes seem to shift as service is being delivered, and service that seemed ideal may be far from acceptable, which is why customers must be specifically asked their opinions of the services. Such customer inquiries can be as simple as "How satisfied are you with the quality of our services?" and "How likely are you to recommend our services to a colleague?"

A recognized technique for measuring service quality, SERVQUAL, based on marketing research, is a perceived service quality questionnaire instrument (see **figure 2**). The SERVQUAL service quality framework compares customer expectations and perceptions of actual performance by asking customers about their expectations and experiences across

five dimensions of quality. The measure of quality is the gap between expectation and experience. If the experience is below expectations, the score is negative. If the experience is above expectations, the score is positive. The SERVQUAL five-dimensions framework is referred to as the Reliability, Assurance, Tangibles, Empathy and Responsiveness (RATER) model,[7] as shown in **figure 2**.

Figure 2—SERVQUAL RATER Model

Dimension	Description
Reliability	Ability to perform service dependably and accurately
Assurance	Ability of staff to inspire confidence and trust
Tangibles	Physical facilities, equipment, staff appearance, etc.
Empathy	Extent to which caring, individualized service is given
Responsiveness	Willingness to help and respond to customer need

For each dimension of service quality shown in **figure 2**, SERVQUAL measures both the expectation and perception of the service on a scale of 1 to 7 (by asking 22 questions in total). Each of the five dimensions is weighted according to customer importance, and the score for each dimension is multiplied by the appropriate weighting. A gap score for each dimension is calculated by subtracting the expectation score from the perception score. A negative gap score indicates that the actual service (the perceived score) was less than what was expected (the expectation score).

The gap score is a reliable indication of each of the five dimensions of service quality. Using SERVQUAL, service providers can obtain an indication of the level of quality of their service and highlight areas that require improvement.

AUDIT FIRM SERVICE QUALITY SELF-ASSESSMENT

Given the increasing importance and growth of the service sector, the quality of service is a key strategic value[8] and has become a strategic instrument for firms since the 1990s.[9] To this end, what follows is a list of questions that audit firms may ask themselves to assess their ability for delivering quality services:

- **Reliability**—Ability to perform promised service dependably and accurately:
  - Does the enterprise deliver the service promised and what its customers believed they were promised every time and under all conditions?
  - Are the exact specifications of the client followed?
  - Is the service performed right the first time?
  - If a response is promised in a certain time, does it happen?
  - Is service timely, consistent, reasonably accurate and dependable?
  - Are statements or reports free of error?
- **Assurance**—Possession of required skill and knowledge to perform service:
  - Does staff possess the right knowledge and skills to deliver the services as promised?
  - Are auditors respectful of customers?
  - Do auditors and staff convey trust and confidence?
  - Can staff provide competent service?
  - Are the materials provided appropriate and up to date?
  - Can staff use the technology quickly and skillfully?
  - Is the service provider trustworthy, believable and honest?
    - Does the audit firm have a good reputation?
    - Do staff members refrain from pressuring the client?
    - Are the responses given accurate and consistent and supported by other reliable sources?
    - Does the organization stand behind its services?
  - Is there security; is there freedom from danger, risk and doubt?
    - Is it safe to enter the premises and to use the equipment?
    - Are documents and other information that are provided to the client held securely?
    - Are use records of clients safe from unauthorized use?
    - Can the client be confident that the service provided was done correctly?
- **Tangible**—Appearance of physical facilities, equipment, personnel, and printed and visual materials:
  - Do the enterprise's physical facilities, equipment and communication materials look attractive and appropriate?
  - Are employees appropriately attired?
  - Are written materials easy to understand and professional?
  - Does technology look modern and functional?
- **Empathy**—Making the effort to know customers and their needs:
  - Does staff provide caring, individualized attention to customers?
  - Is it easy to access staff, services and information?
  - Does someone on staff recognize regular clients and address them by name?
  - Is communication with customers clear, appropriate and timely?
  - Does the enterprise provide services that are appropriate to the individual needs of the customer?

  - Do staff members demonstrate that they understand the customer's needs and situation?
  - Are the client's specific objectives understood?
  - Is the level and cost of service consistent with what the client requires and can afford?
  - Do service providers show politeness, respect, consideration and friendliness?
  - Do staff members have a pleasant demeanor?
  - Does staff refrain from acting busy or being rude when clients ask questions?
  - Are those who answer the telephone (or e-mails) considerate and polite?
  - Does staff observe consideration of the property and values of clients?
  - Does the enterprise listen to customers and acknowledge their comments; are the customers informed in a language that they can understand?
    - When the client contacts the business, will the staff employee listen to the problem and demonstrate understanding and concern?
    - Can staff clearly explain the various options available to a particular query?
    - Does staff avoid using technical jargon when speaking with clients?
    - Does a staff member call if a scheduled appointment will be missed?
- **Responsiveness**—Willingness to help customers and provide prompt service:
  - Is the enterprise willing to help the customer provide prompt service and resolve problems satisfactorily?
  - When there is a problem, does the organization respond to it quickly?
  - Are staff members willing to answer client questions?
  - Are specific times for service accomplishments given to the client?
  - Are public situations treated with care and seriousness?
  - Is the enterprise accessible, approachable and easy to contact? How easy is it to talk to a knowledgeable staff member when the client has a problem?
  - Is it easy to reach the appropriate staff member in person and by telephone and e-mail?

CONCLUSION

The broad quality principle is that each organization should create thorough, controlled procedures for each of its auditing processes. These procedures should deliver quality via processes that are defined, controlled, communicated and used. Understanding and defining processes is essential for establishing benchmarks and to deal with corrective actions when deviations occur. Such processes contribute to the concept of continuous improvement—with the central theme being incremental change to existing processes, implementation of new ways to improve and measure service, and discontinuation of activities that do not add value.

Part 1 of this article examines techniques on how to assess service quality when performing a SAS 70 auditing service. Part 2 describing the development of a multiple-item scale for measuring service quality and how service quality properties can be assimilated into SAS 70 auditing services will appear in volume 4, 2011.

ENDNOTES

[1] *SAS70.com*, "SAS 70 Overview," *www.sas70.com/about.htm*

[2] Bell, T. "Synthesizing SAS 70 Audits and PMI's Project Management Process Groups: Using Project Management Principles to Optimize the SAS 70 Auditing Process," *ISACA Journal*, vol. 4, 2010

[3] Cronin, J.J.; S.A. Taylor; "Measuring Service Quality: A Reexamination and Extension," *Journal of Marketing*, vol. 56, July, 1992

[4] Oliver, R.L.; "A Cognitive Model of the Antecedents and Consequences of Satisfaction Decisions," *Journal of Marketing Research*, vol. XVII, November, 1980

[5] Buttle, F.; "SERVQUAL: Review, Critique, Research Agenda," *European Journal of Marketing*, vol. 30, issue 1, 1996

[6] Turk, Z.; Mutlu Yuksel Avcilar; "The Effects of Perceived Service Quality of Audit Firms on Satisfaction and Behavioural Intentions: A Research on the Istanbul Stock Exchange Listed Companies," *Research Journal of Business Management*, vol. 3, issue 1, 2009

[7] Parasuraman, A.; V.A. Zeithaml and L.L. Berry; "SERVQUAL: A Multiple-item Scale for Measuring Consumer Perceptions of Service Quality," *Journal of Retailing*, vol. 64, issue 1, 1988

[8] Lewis, B.R.; J. Orledgi; V.W. Mitchell; "Service Quality: Students' Assessment of Banks and Building Societies," *International Journal of Bank Marketing*, vol. 12, issue 4, 1994

[9] Donnelly, M.; M. Wisniewski; J.F. Dalrymple; A.C. Curry; "Measuring Service Quality in Local Government: The SERVQUAL Approach," *International Journal of Public Sector Management*, vol. 8, issue 7, 1995

General Auditing for IT Auditors

Danny M. Goldberg, CISA, CGEIT, CIA, CPA, is the professional development practice director at Sunera, an international advisory services firm. Prior to joining Sunera in January 2011, he founded SOFT GRC, an advisory services and professional development firm. Goldberg has more than 14 years of audit experience in the Dallas Fort Worth (Texas, USA) area, including five years as a chief audit executive (CAE)/audit director at two diverse companies. He has the rare experience of being an integral part of, or leading, year-one US Sarbanes-Oxley Act compliance efforts at three companies. Additionally, Goldberg has assisted in leading the establishment of three internal audit/ US Sarbanes-Oxley Act departments.

At times, there seems to be a disconnect between the internal audit and IT audit professions. In terms of assessment of risk, coordination, integration of audit approaches, etc., there is an inherent gap in the approaches of each profession. This gap is very evident, and a general lack of understanding where IT audit fits into the overall audit process is a problem with the segregation of audit approaches.

As companies continue to struggle with the recession, auditors seem to be on a permanent diet—auditors are stretched thin. As the field continuously evolves, chief audit executives (CAEs) will continue to look for cross-trained auditors—those who have the ability, training and experience to perform financial, operational and IT audits, possibly even simultaneously. Furthermore, the industry seems to be tending toward integrated, cross-trained IT and general audit teams. Thus, all IT auditors should understand the process and be able to increase their contribution to the overall audit approach.

This article focuses on the general (i.e., financial, controls and operational) audit process, where IT fits into this process and how to bring it all together.

THE ROLE OF IT AUDIT

The primary role of the internal IT audit staff is to independently and objectively assess the controls, reliability and integrity of the company's IT environment. These assessments can help maintain or improve the efficiency and effectiveness of the institution's IT risk management, internal controls and corporate governance. Internal auditors should evaluate IT plans, strategies, policies and procedures to ensure adequate management oversight. Auditors should make recommendations to management about procedures that affect IT controls.[1]

FINANCIAL, OPERATIONAL AND COMPLIANCE AUDITING

IT auditing plays an integral role in financial, operational and compliance auditing; however, the purpose of each approach is different, as explained in the following sections.

Financial Auditing

A financial audit, or, more accurately, an audit of financial statements, is a review of an enterprise's financial statements that results in the publication of an independent opinion on the relevance, accuracy, completion and fairness (RACF) of the presentation of the financial statements. Internal audit does not opine on the company's financial results, but performs substantive tests on financial balances to verify RACF. Through substantive auditing, auditors gather evidence of the completion, validity and/or accuracy of account balances and underlying transaction classes. Confirmation of cash balances, vouching (going from the general ledger to the invoice/proof of purchase) additions to the fixed asset ledger and review of compliance with debt covenants are all examples of substantive testing.

IT auditing is an integral part of this audit approach. The audit team analyzes, reviews and tests the systems; passing the tests decreases the audit's associated risk. A dependable system encourages the auditor to feel confident in its processes and procedures; the numbers become more reliable.

Operational Auditing

Operational auditing is the process of reviewing a department or other unit of a business or governmental or nonprofit organization to measure the effectiveness, efficiency and economy of operations. It is an evaluation of management's performance and conformity with policies and budgets. In this approach, the enterprise and its operations are analyzed, including appraisal of structure, controls, procedures and processes. The objective is to appraise the effectiveness and efficiency (E&E) of a division, an activity or an operation of the entity in meeting organizational goals.

In today's challenging economic environment, operational auditing is becoming more and more important. Why? Operational auditing, as described here, reviews a process for E&E that can be a great asset to a company, allowing internal audit to be viewed as a revenue generator/cost reducer rather than an overhead cost.

When assessing the E&E of a process, it is important to review the IT systems. An antiquated system can significantly affect E&E. Furthermore, nonoptimized system usage hampers the process's efficiency. For example, if an enterprise installs a new cost management system, but does not activate all the system's control enhancements, the process will remain manual and inefficient.

Compliance Auditing

A compliance audit is a comprehensive review of an organization's adherence to regulatory guidelines. What is examined in a compliance audit will vary depending upon whether an enterprise is a public or private company, what kind of data it handles, and whether it transmits or stores sensitive financial data. For instance, US Sarbanes-Oxley Act requirements designate that the entity must utilize an IT control framework (e.g., COBIT) as a foundation for IT systems and processes. Health care providers that store or transmit electronic health (e-health) records, such as personal health information, are subject to US Health Insurance Portability and Accountability Act (HIPAA) requirements. Financial services companies that transmit credit card data are subject to Payment Card Industry Data Security Standard (PCI DSS) requirements.[2]

IT auditing plays a significant part in compliance auditing. As previously indicated with financial and operational auditing, IT controls and processes are part of compliance, and these pieces are integrated into the overall compliance plan. IT audit must be involved in all facets of compliance auditing.

DIFFERENCES IN APPROACH

The main differences among financial, operational and compliance auditing are:

- The purpose of the audit
- Inclusion of nonfinancial areas
- Cost/benefit vs. verification

As stated previously, the purpose of each audit varies greatly. Financial auditing verifies that the numbers in the financial statements are reported accurately. Compliance auditing reviews adherence to regulations and rules. Operational auditing reviews processes for E&E. In most cases, compliance and operational auditing are pretty much the same process, but operational auditing takes the next step and focuses on E&E. Financial audits, as their name denotes, focus on an enterprise's financial results. On the other hand, compliance and operational audits can focus on hidden numbers and costs that could be reduced—once more demonstrating a strict focus on adherence, efficiency, effectiveness and improvement of the process. In a nutshell, financial audits focus on verification of the reported numbers, operational audits focus on cost vs. benefit, and compliance audits focus on strict adherence to rules and regulations.

ASSESSMENT OF RISK

The audit[3] risk assessment[4] is the stage in the audit planning process in which an auditor[5] determines the likelihood of audit risk.[6] This, in turn, is defined as the possibility of recording an inappropriate opinion on an audit because of a misstatement in the documents examined. An audit risk assessment is the beginning piece used to manage the integrity of an audit and to determine when and how audits should be conducted and by whom.

The IT component is an integral part of the assessment. Either a separate IT assessment or, more appropriately, an integrated assessment, should be completed. The IT component can significantly drive the overall assessment.

In terms of financial auditing, the key financial system's reliability directly, with an inverse relationship, affects the amount of testing necessary. The more reliable a system, the less testing (both IT and general) is necessary. Conversely, in unreliable systems, a significantly greater amount of testing is necessary. If the IT general controls for a system are not reliable, all of the controls must be substantively tested. For example, if access security cannot be relied upon, all access to the system must be tested throughout the year.

IT plays a key role in the assessment of risk both in the planning stage of the audit year and in each audit. With a more reliable system comes less inherent risk in the audit. Additionally, during the preliminary work of an audit, IT contributes to a deeper, more specific review prior to fieldwork.

PRELIMINARY WORK

Basically, preliminary work is everything that the audit team does to set the foundation of the audit and prepare for an efficient and effective audit process. Preliminary work includes the following steps:

1. **Audit objectives**—Determine the reason(s) for performing the audit and the specific goals that the enterprise intends to meet.
2. **Knowledge gathering**—Gather any knowledge relevant to the audit, including prior-year audit files, policies and procedures, narratives, and audit reports issued.
3. **Authoritative research**—Refer to relevant knowledge on the subject matter of the audit in general, including guidance from ISACA and The Institute of Internal Auditors (The IIA), industry guidance, and best practices on the area under review.
4. **Management interviews**—Conduct interviews to garner the scope and assist in creating the risk assessment for the audit; this is a key part of preliminary work.
5. **Internal controls**—Identify current internal controls; this is important to establish a control baseline for the area/division under review.
6. **Walk-throughs**—Take a sample through the process under review to determine whether the process is functioning as intended; walk-throughs are integral to verifying controls and process details.
7. **Preliminary risk analysis**—Develop this through all of the previously mentioned steps; this guides the audit as to where resources should be focused.

Throughout the preliminary work, IT plays an integral role in the assessment of risk. Many auditors separate general and IT audits, a practice that is hard to comprehend. The preliminary process should be completed concurrently for both audits, as the steps can significantly overlap. Regardless of the audit type, all of the steps of preliminary work are necessary for each, either separately or as an integrated audit approach. Excluding IT from a general audit or *vice versa* would limit the knowledge of the audit and audit process and, consequently, limit the effectiveness of the audit approach.

> "Regardless of the audit type, all of the steps of preliminary work are necessary."

AUDIT FIELDWORK

As discussed previously, IT audit and general audit must work hand in hand with each other to complete an efficient and effective audit. The main area in which this will occur is during audit fieldwork.

Audit fieldwork is the process of actually performing the audit. This includes:

- Requests for documents
- Additional and more in-depth interviews
- Completion of audit work program steps (testing)
- Documentation of audit work
- Supervisor review

Audit fieldwork is arguably the most important step of the audit process. This is the step in which the actual work is completed, conclusions are created and supported, and the substance behind the audit report is completed.

Once more, the fieldwork for both the general audit and IT audit should be completed concurrently because there is overlap in the areas and because issues identified could affect the audit approach. In many cases, general auditing and IT auditing are not completed concurrently. For example, if security on a key system is tested and deemed ineffective, substantive procedures may have to be conducted to verify that significant issues or findings did not occur.

CONCLUSION

The world of auditing is moving toward a more integrated approach to the internal audit. The importance of a comprehensive approach to auditing and of auditors becoming

more well rounded and learning all facets of the audit process will continue to be key to departmental and personal growth.

IT auditors should continue to further their ability to conduct general audits and financial, operational or compliance audits. As the industry continues to evolve, the strict line between audit specialties will continue to dissolve because separating each audit approach is neither efficient nor effective. An integrated audit approach will help all types of audit teams gain effectiveness as each audit plays off the other. Accordingly, all auditors should continue to enhance their skill sets and step out of their comfort zones. This will make for better auditors and give these professionals the experience to conduct better audits.

ENDNOTES

[1] Federal Financial Institutions Examination Council (FFIEC), "Audit Booklet," *Information Technology Examination Handbook*, USA, 2003, *www.ffiec.gov/ffiecinfobase/booklets/audit/audit.pdf*

[2] *SearchCompliance.com*, "What Is a Compliance Audit?," 15 January 2009, *http://searchcompliance.techtarget.com/definition/compliance-audit*

[3] Smith, S.E.; "What Is an Audit?," wiseGEEK, *www.wisegeek.com/what-is-an-audit.htm*

[4] Crystal, Garry; "What Is Risk Assessment?," wiseGEEK, *www.wisegeek.com/what-is-risk-assessment.htm*

[5] Tatum, Malcolm; "What Is an Auditor?," wiseGEEK, 19 January 2011, *www.wisegeek.com/what-is-an-auditor.htm*

[6] Sernel, Kimberly; "What Is an Audit Risk?," wiseGEEK, *www.wisegeek.com/what-is-an-audit-risk.htm*

Math on Malware

Henk-Jan van der Molen is a freelance teacher of business intelligence, information security and change management at the Wageningen University (The Netherlands). He can be reached at *henk.jan.van.der.molen@hswageningen.nl.*

The behavior of networks has been studied for a long time, but this knowledge is now more relevant than ever. In a 1998 research paper on computer viruses,[1] Steve White concluded that, in the 10 years prior to the paper's publication, antivirus technology had been successful for known viruses, but some significant problems for further investigation remained. One of these problems was that the then-current model for spreading computer viruses did not seem to match the practice.

As this article will show, the malware[2] problem is already serious, and it is likely that the situation will deteriorate further. The purpose of this article is to use the insights of network theory in the discussion of how the malware problem can be reduced. With a simple network model, the impact of the following commonly used security measures can be evaluated mathematically against the spread of malware:

- Antivirus (AV) software
- Incident and change management procedures
- Security knowledge and awareness
- Conditions for working from home
- A periodic reset of software
- Implementation of different software compartments

TYPES OF NETWORKS

A network is a set of nodes that may be interconnected. Such networks are sometimes also called "graphs." Research may focus on the properties of individual nodes, but this knowledge devalues if the network contains many nodes, as the Internet does. The examination of a large network mainly provides statistical properties with which its behavior can be better understood and predicted.

There are different types of networks. The behavior of computer networks (e.g., links on web pages), biological networks (e.g., predator-prey relationships) and social networks (e.g., calling patterns) may also be relevant for technological networks such as the Internet with its billions of nodes (i.e., servers, clients, routers). The Internet is designed to be robust against a random failure of nodes. However, the Internet is vulnerable if nodes are attacked in descending order of their number of links to other nodes.

E-mail, peer-to-peer (P2P) computing and web browsing form a social network. The size of a social network is difficult to estimate, but the concept "six degrees of separation"[3] (within a small number of steps, everyone knows everyone), also known as the "small-world effect," proves that it is highly interconnected.

Malware can spread via both the Internet and in-person social networks. An Internet worm can infect an online server or workstation without any user interaction, or a user can unintentionally infect a computer with malware by downloading and using an infected file.

DIFFERENT PROCESS MODELS

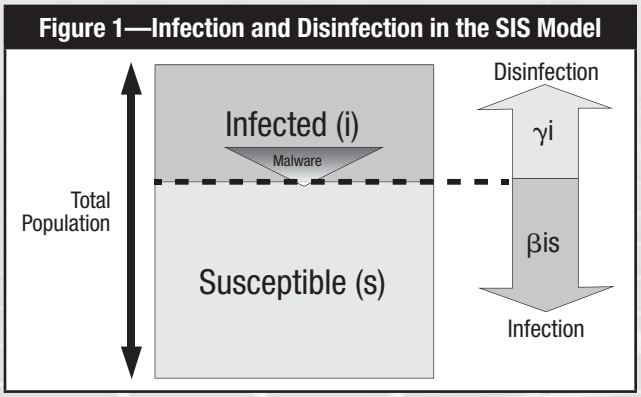
Using the results of previous research,[4, 5] three simple network models are compared. These models are not entirely realistic because they all assume that an infection is "evenly divided" over the network, when, in fact, the topology of the network determines which nodes can transmit malware to other nodes (the upcoming section Injection of Malware provides more details on this). The three network models are:

1. **Percolation theory**—This model is mainly used for capacity calculation and designates nodes and links as either "free" (failure) or "busy" (operational). This model is not appropriate for malware because a computer can be simultaneously infected by multiple exploits, and yet remain operational.
2. **The Susceptible, Infected, Recovered (SIR) model**—The simplest model for the spread of a disease is based on three states (susceptible, infected and recovered) that a single node may go through sequentially. This model can describe the spread of a zero-day computer virus when the used vulnerability in the software was patched after infection and the virus was cleared. Despite patching, there will always remain vulnerabilities in the software.

Because a computer can be infected more than once by the same malware or simultaneously infected by different malware, the SIR model is less suitable to describe the spread of malware.

3. **The Susceptible, Infected, Susceptible (SIS) model**—This model has two states: susceptible and infected (see **figure 1**). Not all diseases result in immunity for survivors, so a node can be reinfected after healing. For example, this applies to tuberculosis and malware that exploits vulnerabilities that are not patched. Therefore, for the purposes of this article, the SIS model was chosen to investigate the spread of malware.

Figure 1—Infection and Disinfection in the SIS Model



DESCRIPTION OF THE SIS MODEL

The SIS model divides the population into two parts: infected (i) and the rest (s), which are susceptible to this infection.

The SIS model indicates that, at first, the infection grows slowly because there are few infected computers that can transmit the infection. In the final phase, the infection slowly reaches the maximum because the probability decreases that an infected node can contact an uninfected node. Therefore, infection growth is proportional to the product.

The number of infected computers is reduced by the detection and removal of malware. This decrease is proportional to the number of infected computers (i). The following formulas describe the SIS model.

Formula 1: $\partial i / \partial t = \beta is - \gamma i, \quad i + s = 1$

The expression ($\partial i / \partial t$) represents the increase of the infection (∂i) in time interval (∂t). The contamination factor (β) is the probability per contact that an infected node can infect a susceptible node, and it also reflects the effectiveness of the deployed preventive security measures, e.g., automated patching and secure software configuration.

The probability of the "resuscitation" of an infected node (γ) also determines the average infection duration ($D = 1 / \gamma$), indicating the effectiveness of the detective and corrective measures.

The solution of formula 1 is the logistic function[6] or S-curve (see **figure 3**).

An important indicator is the basic reproduction number: R_0 ($= \beta / \gamma$), the expected number of new infections from a single infection. By filling in (R_0) in formula 1, the maximum number of infected computers (i_{max}) can be determined when, in the final phase, ($\partial i / \partial t$) drops to zero.

Formula 2: $\partial i / \partial t = \beta is - \gamma i = \gamma i(R_0.s_{min} - 1) = 0 \rightarrow$
$R_0.s_{min} = 1 \rightarrow 1 - i_{max} = 1 / R_0 \rightarrow$
$i_{max} = 1 - 1 / R_0$

Research on the SIS model shows that there always remains some risk of infection, regardless of the value of (β). In the steady state, the force of the infection ($F = \beta.i_{max}$) is at maximum and equal to ($\beta - \gamma$). When the product ($R_0.s$) is smaller than one, the infection dies out. However, if ($R_0.s$) is greater than one, the infection in the population grows.

THE MALWARE PROBLEM

The battle between cybercriminals and security vendors is at full throttle. Recent studies show that even with up-to-date malware signatures, the detection rates of AV software over time have dropped to approximately 40 percent of new malware.[7, 8] Due to the backlog of signature updates and targeted attacks, AV software generally detects only malware that is older than four weeks. Because all AV products show about the same time lag behind malware, malware detection is only marginally improved by deploying multiple virus scanners simultaneously. Also, more virus scanners will produce more potential false positives.

Although modern AV software can sometimes detect malware even when its signatures are unknown, the added value of these heuristic techniques is limited. AV software cannot produce many false positives because, after a short time, the average user will begin to ignore these warnings. Moreover, both closed-source software and malware are often wrapped in encrypted ZIP files, making malware detection much more difficult. Even in 2006, AV software vendor Kaspersky reported, "We're losing this game. There are just

too many criminals active on the Internet underground, in China, Latin America, right here in Russia. We have to work all day and all night just to keep up."[9]

The rapid production and implementation of patches is an absolute necessity, but patches also indicate that software development is not mature. The quality of software can be expressed as the number of errors per 10,000 lines of code. Due to the increasing computer capacity, more complex applications with tens of millions of lines of code are developed and used. At the same time, as products must go to market faster, there is less time to test them. Even after many patches, there remain enough vulnerabilities in software for malware exploitation.

Sometimes, software companies have such a backlog on the development of patches that so-called zero-day exploits can circulate for months before the vulnerability is patched.[10] To make things worse, there are indications that cybercriminals can reverse engineer patches into malware. For instance, using a patch that repairs a buffer overflow, it takes about 30 seconds to generate a malicious input file that triggers the buffer overflow in unpatched computers.[11] This puts slow-patching organizations even more at risk. Worse still, some organizations have a delay in the implementation of patches. Their computers can be infected by malware misusing vulnerabilities for which patches have been issued long ago. Therefore, good change management procedures have a positive effect on security.

The malware problem continues to grow rapidly. For instance, Symantec created 2,895,802 new malicious code signatures in 2009. This represents 51 percent of all malicious code signatures ever created by Symantec.[12] The number of new exploits can be that large because there are "one-click" virus kits readily available on the Internet for little or no money and because the same malware can be encrypted using unique keys. Due to the large amount of malware in circulation, a computer can already be infected with various exploits before the infection is noticed. If the disinfection does not remove all malware, it lowers the value of (γ). Incident management procedures should, therefore, rely on a proven incident response plan. This improves the effectiveness of a disinfection because the need to reinvent in stressful conditions becomes unnecessary.[13] Optimal procedures for incident and change management are, therefore, reflected in a reduced number of and impact from malware incidents.

Cybercriminals earn more money when (β) is high and (γ) is low (see **figure 2**). In this way, more computers are infected (i_{max}) and the infection lasts longer. Yet, it can also be advantageous for cybercriminals to let infections grow slowly and unnoticed because fast-growing malware infections appear on the radar of AV software vendors. By varying the contamination rate (not every malware contact with a susceptible computer leads to an infection), three scenarios have been defined and are discussed in the following section (see **figure 3**).

Figure 2—Battle Between Cyberattack and Cyberdefense

	Security Against Malware (Reduce R_0)	Cybercriminal Actions (Increase R_0)
β	Prevent infection: • Intrusion prevention system, firewall • Heuristic AV software for on-access scanning • Legal, "white-list" software • Configuration: restricted user rights, hardened systems, good passwords, etc. • Implementation of software compartments • Good procedures for changes/updates • Increase in security knowledge and awareness • Preventive security audits	Increase risk of infection by malware: • Multiple attack patterns in malware • Web site offers of customized malware • Social engineering • Sharing of knowledge and malware code • Testing of malware with AV software • Fuzz testing of software for vulnerabilities • Massive and rapid spread of malware • Encryption, code obfuscation • Targeted malware ("precision ammo")
γ	Improve disinfection (detection + correction): • Multiple AV packages for scheduled scans • Intrusion detection system (IDS), logging • Management procedures for incidents and changes, including an incident response plan • Increase in knowledge and awareness • Postmortem security audits	Reduce loss of infected computers: • Root kits, stealth malware, encryption • Malware updates faster than AV software • Imitation of legitimate software, such as AV • Malware self-activation under certain conditions • Patching of infected computers • Use of rotating web servers

DIFFERENT SCENARIOS

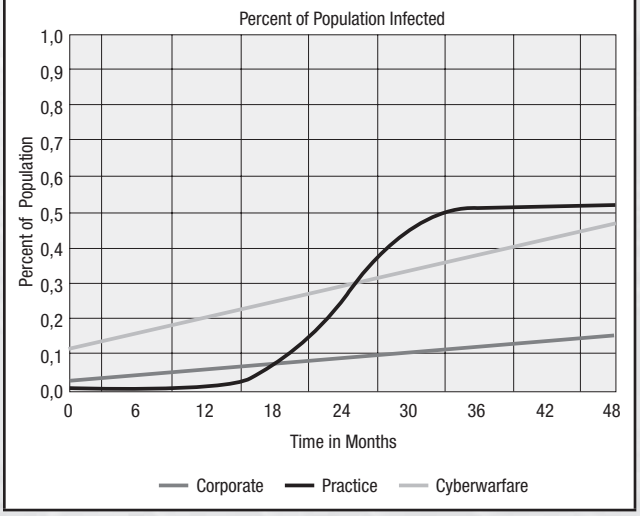
The "corporate" scenario is based on available statistics on malware infections in organizations. Based on the measured effectiveness of AV software for new malware and two consecutive annual surveys on cybercrime,[14, 15] the parameters of the SIS model (β, γ) are calculated.[16] Because the scope of

this research is limited to organizations, this scenario is not representative for the whole population.

The "practice" scenario reflects the common practice to infect as many computers as possible in a short time.[17] For this scenario, few reliable statistics are available. Large-scale infections do appear on the radar of AV software vendors, but that does not mean that the malware can be rapidly eliminated. The experience with the Conficker worm has made that clear.[18]

In the unlikely "cyberwarfare" scenario, the chosen (fictional) parameters are very low so that it takes a lot of time to infect many computers.[19] This scenario can become real only if the exploited vulnerabilities can be abused over a long period of time, and for that, malware knowledge of closed source code is needed or logic bombs need to be planted in computer systems. To avoid detection of the malware, it is essential that the infection not be spread widely so that the abused vulnerabilities are not picked up by the system users, other cybercriminals, AV software vendors or software manufacturers.

Figure 3—Malware Scenarios



PERIODIC RESET OF ALL SOFTWARE

Network theory predicts that, when the nodes with the most links are disabled, the function of the network will deteriorate rapidly. Thus, the proliferation of spam and malware is best reduced by engaging the source. However, disabling these sources is difficult because access is often impeded by placing malware servers outside of the cybercriminal's home country and cybercriminals routinely use rotating web servers to control their botnet.

While malware sources are difficult to control, it remains possible to periodically reinstall clean software on computers, which replaces infected computers with uninfected ones. The security improvement of replacing all the software can be determined by adjusting the SIS model. Let (μ) be the average part of the population in which clean software is installed per month. Combining (μ) with the outflow of (un)contaminated computers (μi + μs) in formula 1 gives:

Formula 3: $\partial i / \partial t = \beta is - i(\gamma + \mu)$

Although this measure reduces the factor (R_0), the security improvement is small if (μ) is much smaller than (γ), as in the replacement of PC hardware, usually every four years. In the "corporate" scenario mentioned previously, the steady state of malware infections drops almost to zero if clean software packages are installed each year.[20] The reset of all computer software is a measure to include in the incident response plan. However, such labor-intensive operations are efficient only when automated.

KNOWLEDGE AND SECURITY AT HOME

To increase productivity, the public's trust (due to privacy) and operational IT systems are vital. A lesser impact of malware means fewer economic damages and more profit. It is a fact that employees cause many incidents. Personal computers of employees at home are often linked directly to business computers by e-mail and Universal Serial Bus (USB) drives. For example, if employees edit business documents on infected personal computers (PCs) at home, the information being edited could be disclosed.

The population of computer users can be divided into two parts: one with sufficient security knowledge and the other with little security knowledge. Because the SIS model becomes complex in heterogeneous populations, the quantitative analysis is not complete.[21] Generally, the group of inexperienced users is larger than the group of security experts, and some business computers (e.g., small to medium-sized enterprises [SMEs]) are insufficiently protected.[22]

On average, a computer user knows little about security. For security experts, the risk of infection by malware (β) is lower and the probability of a successful disinfection (γ) is greater than for security illiterates because the experts,

generally, work more safely and have better technical security. However, when inexperienced computer users suffer more frequently and longer from malware infections, this also affects the computers of security experts and enterprises using the same software. This is because malware can be exchanged between users.

When the security knowledge and awareness of inexperienced users is improved, the impact of malware for the entire population significantly decreases, especially when combined with the reinstallation of clean software, as mentioned previously. This does not mean that everyone has to become a security expert. With a periodic security lecture for personnel that states what should and should not be done, including how to secure home PCs, employees quickly become wise about using the Internet. For example, an important rule of thumb is not to start using new software immediately. If, four weeks after the download, the updated AV software still does not find malware in the (quarantined) downloads, it is far more likely that the downloads are actually free from malware. Additionally, some enterprises impose rules for working at home and provide employees with business software and security software for free. Enterprises that select freeware or open-source software as standard products avoid the extra license costs for private usage.

Experts can assess the effectiveness and efficiency of the implemented security measures. If the security is properly designed and implemented, inexperienced users cannot easily infect their PCs. If employees know why their access rights are limited and why business software is white-listed, and if the lessons learned from incidents are widely communicated, support is created and security awareness improves. Even so, the malware risk remains at maximum for security experts and enterprises using market-leading software.

SOFTWARE COMPARTMENTS

All software contains vulnerabilities, and computers that use the same software share the same vulnerabilities. For malware, all computers using the same software form a separate population. For example, Windows PCs are a software compartment separated from the Mac OS and Linux compartments. While software compartments may be linked by common code for hardware drivers and network functions, in practice, it is unlikely that Windows malware can infect a Mac. This is because there is little shared source code, which has often been rigorously reviewed to eliminate vulnerabilities.

The larger the population, the more attractive it is for cybercriminals to develop exploits that misuse the vulnerabilities in that population. To maximize their profits, cybercriminals are targeting their malware on the (generally used) software with the largest market share.[23] Although it is possible to write malware for a Mac or a Linux PC, at the same costs, Windows malware is much more profitable because of its higher market share.

Generally, monopolies have been proven to be vulnerable, and software monopolies are no exception to this rule: The probability for malware to infect a computer using this software is the greatest. Therefore, it is obvious that the economics of malware can be reduced by creating more software diversity. To enable this, enterprises must abandon the idea that the interchangeability of information depends on using the same software. Instead, enterprises must dare to rely on data standards to break vendor lock-in. The use of open standards also ensures that data in electronic archives can still be processed in the future.

The SIS model can predict the effect on the spread of malware if the software population is made more diverse. Suppose that (q) is the part of the population that becomes immune to the malware targeting the market-leading software by migrating to alternative software. If the value of (q) does not affect the software monopoly, the vast majority of malware continues to target the market-leading software used by the rest of the population (1 - q). By replacing (i + s = 1) with (i + s + q = 1) in formula 1, the infection rate is decreased:

Formula 4: $\partial i / \partial t = \beta is - \gamma i = \beta i(1 - i - q) - \gamma i$

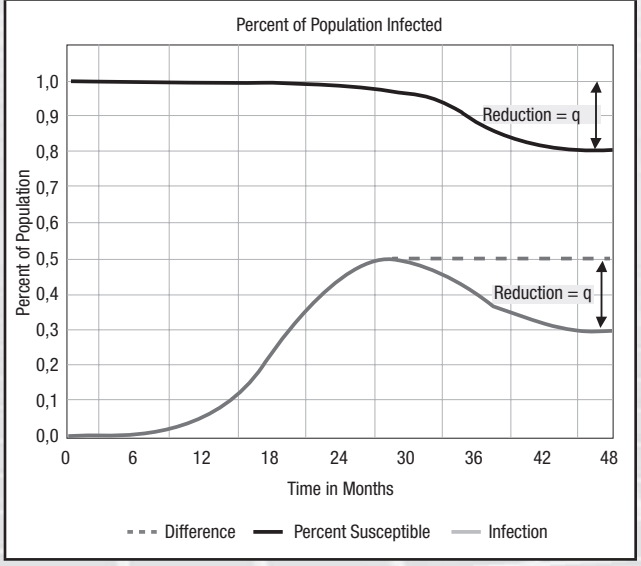
By creating more software diversity, malware focused on market-leading software will spread more slowly because of the decrease in fertile contacts, as expressed by the term (βiq). This creates more reaction time for the software industry to respond to new malware. The number of infections in formula 2 is also reduced:

Formula 5: $R_0.s_{min} = 1 = R_0 (1 - i_{max} - q) \quad \rightarrow$
$i_{max} = 1 - q - 1 / R_0$

Therefore, the number of infections in the steady state will be reduced by (q), the same as the reduction in susceptible computers. If (q) is greater than or equal to the (i_{max}) of a

malware variant, then this malware dies out. Even if (q) is smaller than (i_{max}), the resulting new value of (i_{max}) is lower than the proportional decline of susceptible computers (1 - q). The effect of software compartments is shown graphically in **figure 4**.

Figure 4—The Effect of Software Compartments



Therefore, the force of the infection ($F_{max} = \beta i_{max} = \beta - \gamma - \beta q$) decreases with ($-\beta q$) for the whole population. If there is only one software compartment, $F_{max} = (\beta - \gamma)$, so by increasing software diversity, the force of the infection is reduced even within the susceptible (1 – q) subpopulation:

Formula 6: $F_{max} = \beta i_{max} / (1 - q) = (\beta - \gamma - \beta q) / (1 - q) = \beta - \gamma - \gamma q / (1 - q)$

Suppose that the population is divided in two software compartments, in which software A has an 80 percent market share and software B has 20 percent. It is easy to see that (q = 0.8) for the compartment B. In other words, an infection that focuses on compartment B cannot easily spread and, most likely, will die out quickly. Computers using software B are likely infected only by injection of malware, hardly by mutual contacts. This result disproves the often-heard statement that switching from market-leading software does not increase security. Only in the unlikely event that the new software reaches the market shares of the old market leader, will the malware situation be more or less the same. The more software diversity that exists within a population, the more the propagation of malware is disturbed.

This calculation also shows the effects of more software standardization. By replacing the term (-q) with (+q) in formulas 5 and 6, it becomes clear that (i_{max}) and the force of the infection (F) will increase. In the real world, this means that populations that continue to use market-leading software will suffer more damage due to cybercrime than populations that switch to other standard products. However, a necessary precondition to eliminate vendor lock-in is the adaptation of open standards.

INJECTION OF MALWARE

The SIS model assumes that infections are spread evenly across the network, but this is the case only if the malware has been spreading for some time. Therefore, the model cannot be used to describe the injection of new malware in the population because, for that, the topology of the network is essential. This includes the distribution of worms and malware from Web servers (drive-by exploits). The more links a malware source has, the greater the probability that the infection can spread. Suppose that the number of nodes with a direct relationship to a malware source is equal to (k). If (n) is the total number of susceptible computers, the probability (p) that a malware source can transfer a new exploit (j) is:

Formula 7: $p_j(\text{first infection}) = \beta_j \sum_m k_m / n \quad \rightarrow \quad p_j$
$(\text{NO first infection}) = (1 - \beta_j \sum_m k_m / n)$

Here (k_m) is the number of connections of the malware source node (m). The index (m) indicates that cybercriminals can use multiple sources simultaneously to spread exploit (j).

The probability that a malware source can infect a susceptible node is also equal to the expected proportion of the population that the source can infect directly. The proportion of the population that is not infected is the product of all the probabilities (designated by $\prod_c$ in formula 8) that each individual exploit fails to infect a susceptible computer.

Suppose that every month (c) new exploits are released. The proportion of the population that is directly infected by one or more of these new exploits is (again, switch to the complementary probability):

Formula 8: $\partial i_c / \partial t = 1 - \prod_c (1 - \beta_j \sum_m k_m / n)$

Formula 8 can be simplified to (βcv) with the following assumptions:

- (β) is roughly the same for all exploits, choosing the practice scenario.
- The spreading factor ($v = \sum_m k_m / n$) is equal for all malware source nodes and $v << 1$.

To infect as many computers as possible in a short time, cybercriminals link their malware to popular (hacked) web sites, which have a high value for $\sum_m k_m$. Although the 240,000 new exploits per month that Symantec has created (= c) is small compared to the billions of Internet nodes (n), this strategy provides the best way to infect many computers as quickly as possible.

It is also possible to spread malware using a two-stage process, using infected computers in a botnet to send spam messages containing malware. With 100 billion malware messages per day,[24] if only one out of every 100,000 recipients of a spam message looks at the "offer,"[25] 2 million computers can be infected and the volume of spam continues to rise.

The effect of diversification is that only the (1 - q) part of the population using market-leading software is susceptible to an injected exploit. Combining this with formula 4, the overall growth of the infections due to the spread of existing infections and new malware becomes:

Formula 9: $\partial i / \partial t = \beta i(1 - i - q) - \gamma i + \beta cv(1 - q)$

Thus, software diversification makes sense for both the initial infection and the spread of existing malware because the term (q) is present in both the rate and extent of the infection.

CONCLUSION

The malware risk is expected to increase in the near future, especially when cybercriminals routinely start to automatically generate malware from software patches. Such practices will put the security of organizations that want to test patches first under great pressure. Even with optimal security measures, not all malware infections can be prevented. While malware infections result in accumulating economic damages to society, no longer can anyone afford to ignore security measures that are effective against cybercrime.

With the limitations noted, network theory and the comprehensive SIS model provide new insights into the effectiveness of security measures. The small-world effect is a double-edged sword: Any enemy in the digital world is just a few clicks away.[26] Every infected home computer of an employee is just one step away from the enterprise's critical information systems. At the very least, a proven incident response plan is a necessary procedure.

Illegal software often contains malware. When employees regularly work at home, enterprises should impose rules of conduct. Employees can infect business computers by sending e-mail from home or by using USB drives. Enterprises reduce the risk of malware by improving the knowledge of employees with mandatory security training and by providing business and security software for free. Enterprises that standardize freeware or open-source software eliminate the extra license costs for this.

Enterprises can reduce the current risk of malware to almost zero by annually resetting software on each computer. It is also advisable to block nonstandard software on business computers using a white list. Improving the security knowledge of inexperienced users reduces the risk of infection for the whole population, including security experts.

A software monopoly maximizes the economic return of malware. Of course, companies can still choose standard software, but from a cybercrime perspective, it is undesirable that all companies use the same software. Increasing the use of nonmarket-leading software reduces the risk of infection because the number of fertile contacts for malware decreases. A sufficiently high percentage of computers with alternative software can significantly reduce malware infections. This alternative software should preferably use open standards to ensure interoperability, avoid vendor lock-in and provide sustainable access to archived information.

AUTHOR'S NOTE

The author would like to thank Robert Kooij, Ph.D., of the Electrical Engineering, Mathematics and Computer Science faculty at the Delft University of Technology (The Netherlands) for his support.

ENDNOTES

1 White, Steve R.; "Open Problems in Computer Virus Research," Virus Bulletin Conference, Munich, Germany, October 1998, *www.research.ibm.com/antivirus/SciPapers/White/Problems/Problems.html*

2 In this article, the terms "exploits" and "malware" (computer viruses, worms and spyware) are considered synonyms; however, please note that an exploit abuses a vulnerability in software and usually instructs the computer to download and install malware.

[3] Kuperman, Marcelo; Guillermo Abramson; "Small World Effect in an Epidemiological Model," *Physical Review Letters*, vol. 86, no. 13, 2001, *http://fisica.cab.cnea.gov.ar/estadistica/abramson/papers/smallworld/swepi.pdf*

[4] Newman, M. E. J.; "The Structure and Function of Complex Networks," *www-personal.umich.edu/~mejn/courses/2004/cscs535/review.pdf*

[5] Van Mieghem, Piet; Jasmina Omic; Robert Kooij; "Virus Spread in Networks," *www.nas.ewi.tudelft.nl/people/Piet/papers/IEEEToN_virusspread.pdf*

[6] See *www.cs.xu.edu/math/math120/01f/logistic.pdf.*

[7] Staniford, Stuart; "Do Antivirus Products Detect Bots?," FireEye Malware Intelligence Lab, 20 November 2008, *http:// blog.fireeye.com/research/2008/11/does-antivirus-stop-bots.html*

[8] AV-Comparatives e.V., "Anti-virus Comparative—Proactive/Retrospective Test—February/May 2010," *www.av-comparatives.org/images/stories/test/ondret/avc_report26.pdf*

[9] Naraine, Ryan; "The Zero-day Dilemma," *eWeek.com*, 24 January 2007, *www.eweek.com/article2/0,1759,2087034,00.asp*

[10] Leyden, John; "MS Knew of Aurora Exploit Four Months Before Google Attacks," *The Register*, 22 January 2010, *www.theregister.co.uk/2010/01/22/aurora_exploit_known_months*

[11] Brumley, David; Pongsin Poosankam; Dawn Song; Jiang Zheng; "Automatic Patch-based Exploit Generation Is Possible: Techniques and Implications," *www.cs.cmu.edu/~dbrumley/pubs/apeg.pdf*

[12] Symantec, *Global Internet Security Threat Report Trends for 2009, http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_internet_security_threat_report_xv_04-2010.en-us.pdf*

[13] *Computable,* "Incident management badly needed" (in Dutch), *www.computable.nl/artikel/ict_topics/security/1681630/1276896/incident-management-broodnodig.html*

[14] Ernst & Young, "Results ICT Barometer on Cybercrime" (in Dutch), February 2010, *www.ict-barometer.nl/files-cms/File/Onderzoekresultaten%20ICT%20Barometer%20over%20cybercrime%20op%2024%20februari%202010.pdf*

[15] Ernst & Young, "Results ICT Barometer on IT-security and Cybercrime" (in Dutch), 28 January 2009, *www.ict-barometer.nl/files-cms/File/Rapport%20ICT%20Barometer%20over%20ICT-beveiliging%20en%20cybercrime%20%2028%20%20januari%202009.pdf*

[16] From the AV software research in endnote 10, $\gamma = 0{,}435$; calculated from the $(\partial i/\partial t)$ in endnote 16, $\beta = 0{,}52$

[17] From the AV software research in endnote 10, $\gamma = 0{,}435$; an estimation of $\beta = 0{,}9$

[18] The Rendon Group, "Conficker Working Group: Lessons Learned," USA, June 2010, *www.confickerworkinggroup.org/wiki/uploads/Conficker_Working_Group_Lessons_Learned_17_June_2010_final.pdf*

[19] Fictional parameters for the "cyberwarfare" scenario: $\beta = 0{,}1$ and $\gamma = 0{,}04$

[20] See endnote 18, $\gamma = 0{,}435 + 1/12 = 0{,}518$, $\beta = 0{,}52$; the steady state of malware infections drops from 0,16 to 0,003.

[21] Omic, Jasmina; Robert E. Kooij; Piet Van Mieghem; "Heterogeneous Protection in Regular and Complete Bi-partite Networks (Work in Progress)," International Federation for Information Processing, 2009, *www.nas.its.tudelft.nl/people/Rob/telecom/netw_het.pdf*

[22] This statement is based on the professional experiences of the author.

[23] *Computable*, "Engage cyber crime: Divide and Conquer," (in Dutch), 21 February 2008, *www.computable.nl/artikel/ict_topics/security/2357426/1276896/aanpak-cybercriminaliteit-verdeel-en-heers.html*

[24] Trend Micro, "TrendLabs Global Threat Trends 1H 2010," Philippines, 2010, *http://us.trendmicro.com/imperia/md/content/us/trendwatch/researchandanalysis/tm101hthreat_report.pdf*

[25] Specter, Michael; "Annals of Technology—Damn Spam: The Losing War on Junk E-mail," *The New Yorker*, 6 August 2007, *www.newyorker.com/reporting/2007/08/06/070806fa_fact_specter?currentPage=1*

[26] Murphy's Law of Combat No. 1: If the enemy is in range, so are you.

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*

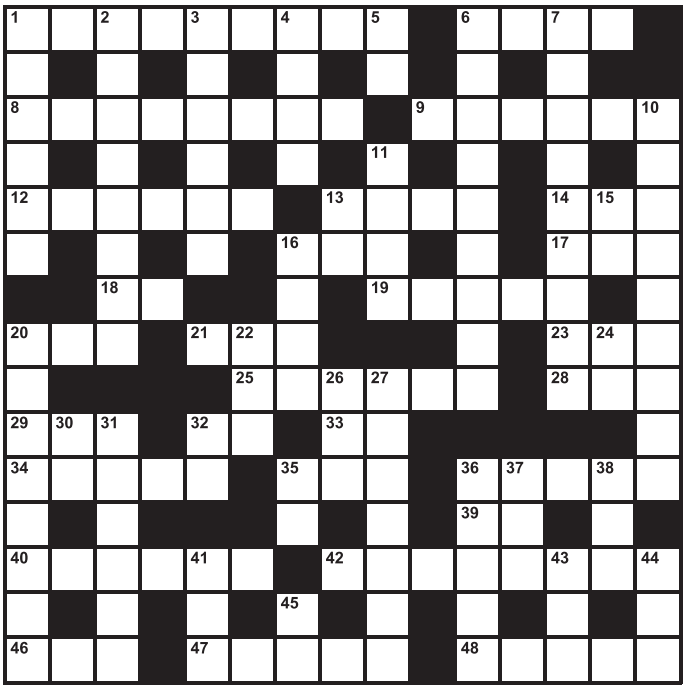
The comprehensive CISM Practice Question Database v11 combines the *CISM Review Questions, Answers & Explanations Manual 2011* with the *CISM Review Questions, Answers & Explanations Manual 2011 Supplement* into a single 750-question study guide. Exam candidates can take sample exams with randomly selected 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

Crossword Puzzle

By Myles Mellor
www.themecrosswords.com



ACROSS
1 Unauthorized entry
6 Combine
8 Excel statistical presentation feature (2 words)
9 Directions of activity
12 Pamper
13 Weakness in a system
14 Testing area
16 Spelling test
17 Self-image
18 Way to improve disinfection: multiple __ packages for scheduled scans
19 ISACA framework used by the EC in its VAST assessment tool
20 Beam
21 Factor in equipment reliability
23 ___ hunch (2 words)
25 Subscribes to
28 Needle
29 Fall
32 Politician, for short
33 Farm animal
34 Act relating to responsibilities for data security for US companies
35 Root ___
36 Type of computing using mass centralization of computer resources
39 Read only, for short
40 Code to gain entry
42 For SEC registrants, US companies will have to report US GAAP and IFRS in _____
46 ____ 70 audit
47 IT control framework
48 Educate

DOWN
1 Have an effect on
2 Commission that formed COSO
3 Support
4 SEC will be converting to these standards in accounting
5 Negative comment
6 System security features
7 "Fraud Auditing and Forensic Accounting," by Tommie and Aaron ___
10 Undermined
11 Map abbr.
13 Symbol for iron
15 Agricultural, abbr.
16 One of the GL tables in the SAP system
20 Warning signs (2 words)
22 Breach
24 Sodium symbol
26 Profit, for short
27 Get data out of a system
30 Roman 2
31 Mentally prepares
32 Master's degree
35 A unit of power equal to 1,000 watts
36 Design
37 Laughter on the Internet, abbreviation
38 Adopt
41 Organization responsible for protecting investors and facilitating capital formation, abbr.
43 Period of leave from study, abbr.
44 Network type
45 Database, abbr.

(Answers on page 54)

HelpSource Q&A

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

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

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

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 Often, I have read articles in which the costs of security incidents are quantified in monetary terms. Can someone really quantify the costs? I believe that many of us do not even log the incidents properly. (I am from the health care industry.) How can we calculate the cost of security incidents, and is there any formula that is readily available and widely followed? On the other hand, how does one compute the cost of compliance?

A I cannot comprehend reports that quantify the costs of security incidents. Maybe it is possible, but I am not aware of a one-size–fits-all formula that can make this happen.

Depending on the industry and the line of business, security incidents can have different ramifications. Various parameters determine the impact on the entity, and there can be different types of incidents, too. For example, a simple fire could cause damage to machinery and equipment. In extreme scenarios, lives may be lost as well. Fire accidents may happen due to a malfunction in the electrical connectivity, with no manual act contributing to the cause. In some cases, incidents can result from sabotage caused by internal or external resources.

Another type of incident would be one caused by logical control failures, e.g., data being stolen or unintentionally left unattended, leading to a compromise. Someone inadvertently mailing data to an unrelated third party can result in an incident that can cause immense damage to an entity.

There is a widely held theory—again, I have not come across a study with due academic rigour to substantiate this—that insiders cause more damage to an enterprise than outsiders. I do not necessarily subscribe to this, as I have yet to see proof with numbers and facts.

Systems and applications becoming unavailable are also classified as security incidents. Nonavailability of systems and applications can lead to crises in which the continuity of business operations can be impacted. In general, external factors cause nonavailability—this is, again, a widely held belief, and I have no numbers available to substantiate it. An undersea cable cut somewhere in Egypt may have potential impact on companies in Manila, if the telecom service providers in the Philippines have connectivity to such cables.

With several types of incidents occurring, how does one attribute a monetary value to the loss, and how does one quantify the loss? I am not ruling out the possibility of quantifying loss, but it is not something that is possible in a straightforward and simple manner.

Let us discuss some of the challenges that impede such calculations.

There are simple cases of physical loss or damage to equipment. Replacement costs and loss of productivity can contribute to the cost of incident calculations.

Major security incidents can lead to a loss of reputation to the institution in which the incident occurred. If a banking site were to be hacked, its online customers might lose confidence and start refraining from doing online banking, or they may change banks altogether. If the customers choose to refrain from doing online banking, they may crowd the branches to complete banking transactions, which would result in delays for customers if the branch were not equipped to service such an extended set of customers. Furthermore, potential new customers who may have been considering opening an account may seek alternate options with other banks. This implies potential loss of future revenue. Hacking of the site may also lead to productivity and actual revenue losses. How does one compute future revenue losses?

Consider the current situation in India where the chief auditor of the government has issued a report indicting various individuals on what are called 'presumptive losses'. The argument placed by the chief auditor is that a notional loss has been caused by adopting the wrong method to sell government-owned resources to private companies.[1] Arguments have been placed against

the approach adopted by the government auditors, and the matter is now in the Supreme Court of India.

Without going into the merits of the case, what is interesting is the concept of computing presumptive losses. How should one do so in the context of information security incidents? The assumptions have to be explicit for one to do such calculations, and any such approach is prone to challenges in terms of acceptance.

The industry regulator or the law of the land may impose certain fines and penalties on the entity. Costs of such payments have to be factored into the calculation.

The biggest question is how to compute the loss of reputation. I have not come across a formula that helps to compute loss of reputation in monetary terms. We have had cases of certain firms ceasing to exist overnight due to controversies. Reputation loss, in some cases, can cause so much damage that the entity may cease to exist. History has a number of examples, including a famous international auditing firm (one among the then-Big Six) that disappeared overnight due to loss of reputation.

An excellent study—slightly older in terms of the time when it was conducted—is available titled 'The Economic Cost of Publicly Announced Information Security Breaches: Empirical Evidence From the Stock Market'. According to the authors, 'this study examined the economic effect of information security breaches reported in newspapers on publicly traded US corporations. We found limited evidence of an overall negative stock market reaction to public announcements of information security breaches. However, further investigation revealed that the nature of the breach affects this result. We found highly significant negative market reaction for information security breaches involving unauthorized access to confidential data, but no significant reaction when the breach does not involve confidential information. Thus, stock market participants appeared to discriminate across types of breaches when assessing their economic impact on affected firms. These findings are consistent with the argument that the economic consequences of information security breaches vary according to the nature of the underlying assets affected by the breach'.[2]

Another study, done in Japan by a different set of academics, is titled 'The Effect of Information Security Incidents on Corporate Values in the Japanese Stock Market'.[3] According to the study, corporate investments on information security are highly evaluated as intangible assets in the stock market, especially for IT-oriented firms. Based on this research, the study concludes that 'firms whose tangible assets are highly evaluated suffer from the security incidents more severely than those whose intangible assets are evaluated smaller'.

Given what has just been discussed, I cannot think of a simple and straightforward formula to compute the cost of security incidents.

On the other hand, all the controls implemented as part of an entity's routine operational risk mitigation processes cannot be factored into compliance costs. Compliance costs must relate only to those cost of controls implemented for the purpose of certain regulatory and legal compliance requirements.

I invite any and all readers who have strong views and believe that there are such formulae out there to write to me and I will share your comments with *Journal* readers.

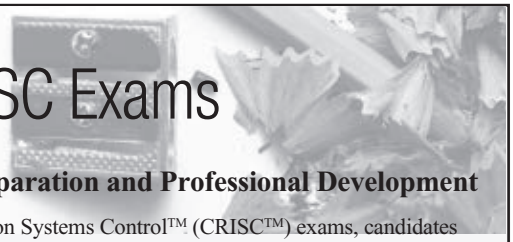
ENDNOTES

[1] Ishiguro, Masaki; Hideyuki Tanaka; Kanta Mantsuura; Ichiro Murase; 'The Effect of Information Security Incidents on Corporate Values in the Japanese Stock Market', Japan, 2006, *http://www.mri.co.jp/PUBLICITY/PAPER/2006/20061023_si304.pdf*

[2] Campbell, Katherine; Lawrence A. Gordon; Martin P. Loeb; and Lei Zhou; 'The Economic Cost of Publicly Announced Information Security Breaches: Empirical Evidence From the Stock Market', *Journal of Computer Security*, vol. 11, no. 3, 2003

[3] *Op cit*, Ishiguro

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

CPE Quiz

Prepared by Kamal Khan,
CISA, CISSP, CITP, MBCS

QUIZ #136

Based on Volume 1, 2011—Virtualization Security, Challenges and Solutions
Value—1 Hour of CISA/CISM/CGEIT/CRISC Continuing Professional Education (CPE) Credit

TRUE OR FALSE

CHAUDHURI, VON SOLMS AND CHAUDHURI ARTICLE

1. Virtualization is a software technology that divides a physical resource into virtual resources called virtual machines (VMs).

2. Network virtualization hides the physical nature of server resources, including the number and identity of individual servers, processors and operating systems (OSs).

3. According to Gartner, 50 percent of virtualized servers will be less secure than the physical servers they replaced through 2012.

4. The most important software in a virtual IT system is the hypervisor. Any security vulnerability in the hypervisor software will put VMs at risk of failure.

5. A Gartner study indicates that by 2012, almost 50 percent of servers will be virtualized throughout the world.

KANDRA, SEWELL AND NYAMARI ARTICLE

6. It is as important to develop and tune soft skills as it is to demonstrate the right knowledge through certifications and have experience with relevant standards, legislation and compliance requirements.

7. The auditor's focus is to be critical of the individual rather than the organizational policies, procedures and process.

8. A KPMG report examining financial services firms in the UK and India highlights the "soft skills gap" by noting that 58 percent of organizations in the UK and more than 62 percent of organizations in India struggle to recruit the right talent.

9. ISACA's Young Professional Subcommittee (YPS) was formed in 2009 to facilitate the development of a community that meets the needs of young professionals.

SOOD AND ENBODY ARTICLE

10. Cross-site Scripting (XSS) worms are self-replicating in nature and spread rapidly on social networking sites because of the interconnection among various profiles.

11. The first step of the model to explain the working of worms occurs when the malware waits for the user to visit and log in to a specific social networking web site.

12. The major factor that contributes to the spreading of malware is user ignorance regarding the technology used on social networking web sites.

13. Users should run unpatched OSs to avoid the exploitation of vulnerabilities in various components of installed software.

HORTON ARTICLE

14. Any business that accepts credit or debit payments is likely required to comply with the Payment Card Industry Data Security Standard (PCI DSS)—measures created in 2005.

15. Members of the National Retail Federation have collectively spent more than US $10 billion so far on PCI DSS compliance as part of their security programs.

DIMITRIADIS ARTICLE

16. Information integrity is a key information security component related to player trust.

17. Architecture represents how security processes are automated by the use of technology.

ISACA Journal

CPE Quiz

Based on Volume 1, 2011—Virtualization Security, Challenges and Solutions

Quiz #136 Answer Form

(Please print or type)

Name _____

_____

Address _____

_____

_____

CISA, CISM, CGEIT or CRISC# _____

Quiz #136

True or False

CHAUDHURI, VON SOLMS AND CHAUDHURI ARTICLE

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

KANDRA, SEWELL AND NYAMARI ARTICLE

6. _____
7. _____
8. _____
9. _____

SOOD AND ENBODY ARTICLE

10. _____
11. _____
12. _____
13. _____

HORTON ARTICLE

14. _____
15. _____

DIMITRIADIS ARTICLE

16. _____
17. _____

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

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

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

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

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

Answers—Crossword by Myles Mellor

See page 49 for the puzzle.

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

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

CCH Teammate	*www.CCHTeamMate.com*	**Inside Back Cover**
CheckAud®	*www.checkaud.com*	**5**
ExamMatrix	*www.www.ExamMatrix.com/ISJ*	**11**
Regis University	*www.RegisDegrees.com/ISACA*	**Back Cover**
Saint®	*www.saintcorporation.com/mac*	**1**
University of Maryland University College	*www.umuc.edu/cyberedge*	**9**

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*.

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

ISSN 1944-1967

Leaders and Supporters

ISACA Bookstore

Resources for your Professional Development

Over 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-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.

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**

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 EDITION

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**

A NEW AUDITOR'S GUIDE TO PLANNING, PERFORMING, AND PRESENTING IT AUDITS

NEW

Nelson Gibbs, Divakar Jain, Amitesh Joshi, Surekha Muddamsetti, Sarabjot Singh

Information technology is a highly dynamic, rapidly changing environment. IT auditors are expected to stay current with the latest tools, technologies, and trends, and may need to do additional research to prepare for specific audits. This book is designed to help aspiring and active internal auditors take a step back and understand the general process and activities involved in conducting an audit around technology.

This book uses a simplified four-layer technology model of networks, operating systems, databases, and applications. It provides easily understandable concepts of the technology environment that can be applied in most organizations with little modification. 2010, 225 pages. **1-IIA**

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 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

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

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 11*g* (differences from previous versions of Oracle Database are noted, as well as differences that may exist based on the host operating system of the database).

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

SECURITY, AUDIT AND CONTROL FEATURES SAP® ERP: TECHNICAL AND RISK MANAGEMENT REFERENCE SERIES, 3RD EDITION

Deloitte Touche Tohmatsu Research Team and ISACA

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

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

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

2009, 470 pages. **ISAP3**

NON-ENGLISH RESOURCES

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

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**

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.

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**

CYBER ATTACKS: PROTECTING NATIONAL INFRASTRUCTURE

NEW

Edward Amoroso

No nation has a coherent technical and architectural strategy for preventing cyber attacks from crippling essential critical infrastructure services. This book initiates an intelligent national and international dialogue amongst the general technical community around proper methods for reducing national risk. This includes controversial themes such as the deliberate use of deception to trap intruders. It also serves as an attractive framework for a new national strategy for cyber security, something that several administrations have failed in attempting to create. This book offers a technical, architectural, and management solution to the problem of protecting national infrastructure. It takes the debate on protecting critical infrastructure in an entirely new and fruitful direction. 2011, 248 pages. **11-EL**

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

NEW EDITION

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 WEB APPLICATIONS, 3RD EDITION

NEW

Joel Scambray

Protect your web applications from malicious attacks by mastering the weapons and thought processes of today's hacker. Written by recognized security practitioners and thought leaders, *Hacking Exposed Web Applications, 3rd Edition* is fully updated to cover new infiltration methods and countermeasures. Find out how to reinforce authentication and authorization, plug holes in Firefox and IE, reinforce against injection attacks, and secure web 2.0 features. Integrating security into the web development lifecycle and into the broader enterprise information security program is also covered in this comprehensive resource. 2010, 482 pages. **23-MHE**

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

NEW EDITION

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**

SECURITY INFORMATION AND EVENT MANAGEMENT (SIEM) IMPLEMENTATION

NEW

David R. Miller, Shon Harris, Allen Harper, Stephen VanDyke, Chris Blask

Written by IT security experts, *Security Information and Event Management (SIEM) Implementation* shows the reader how to deploy SIEM technologies to monitor, identify, document, and respond to security threats and reduce false-positive alerts. The book explains how to implement SIEM products from different vendors, and discusses the strengths, weaknesses, and advanced tuning of these systems. Readers will also learn how to use SIEM capabilities for business intelligence. Real-world case studies are included in this comprehensive resource.
2010, 464 pages. **24-MSIEM**

SYSTEM FORENSICS, INVESTIGATION, AND RESPONSE

NEW

John R. Vacca, K Rudolph

Computer crimes call for forensics specialists, people who know how to find and follow the evidence. *System Forensics, Investigation, and Response* begins by examining the fundamentals of system forensics, such as what forensics is, the role of computer forensics specialists, computer forensic evidence, and application of forensic analysis skills. It also gives an overview of computer crimes, forensic methods, and laboratories. The book then addresses the tools, techniques, and methods used to perform computer forensics and investigation. Finally, it explores emerging technologies as well as future directions of this interesting and cutting-edge field. 2011, 339 pages. **2-JBSF**

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 EDITION

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**

EMPOWERING GREEN INITIATIVES WITH IT: A STRATEGY AND IMPLEMENTATION GUIDE

NEW

Carl H. Speshock

A straightforward guide to the role of IT departments and vendor's in assisting organizations in going green with the aid of IT-related resources and offerings. This book provides organizations with strategy, planning, implementation and, assessment guidance for their green initiatives. It discusses the many benefits of green initiatives with the assistance, integration and collaboration of the IT department and vendors, i.e., custom and vendor application development and reporting tools, green IT examples and, business intelligence dashboards that can perform analytical and predictive analysis of green related business data. Practical and thorough, this book includes helpful checklists, a glossary and resources to get started with a business's green initiatives. 2010, 235 pages. **89-WEG**

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 EDITION

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**

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 GOVERNANCE: POLICIES & PROCEDURES, 2011 EDITION

NEW

Michael Wallace, Larry Webber

IT Governance Policies & Procedures will help you to devise an information systems policy and procedure program uniquely tailored to the needs of the reader's organization. Not only does it provide sample policies, but this valuable resource provides the information needed to develop useful and effective policies for your unique environment. For fingertip access to the information you need on policy and planning, documentation, systems analysis and design, and much more, the materials in this ready-reference desk manual can be used as models or templates to create similar documents for the reader's own organization. CD-ROM included. 2010, 981 pages. **5-AS11**

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**

IT PROJECT MANAGEMENT: ON TRACK FROM START TO FINISH, 3RD EDITION

NEW

Joseph Phillips

This practical, up-to-date guide explains how to successfully manage an IT project and prepare for CompTIA Project+ certification. *IT Project Management: On Track from Start to Finish, 3rd Edition* walks you through each step of the IT project management process, covering critical strategies for on-time and within-budget projects. You'll get proven methods for initiating a project, selecting qualified team members, conferring with management, establishing communication, setting realistic timetables, tracking costs, and closing a project. CD-ROM included. 2010, 640 pages. **25-MIPM**

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

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**

A PRACTICAL GUIDE TO REDUCING IT COSTS

NEW

Anita Cassidy, Dan Cassidy

Eliminating and driving down costs has long been second nature for many IT organizations. In challenging economic times, even further cutting of IT costs is a requirement for the survival of many organizations. Whether in the midst of an economic downturn or upturn, effective cost management is critical as IT costs can be a significant portion of an organizations overhead cost structure and can even impact an organizations competitive position. *A Practical Guide to Reducing IT Costs* provides a toolkit of innovative ideas to assess and reduce costs in an IT organization. It outlines a compilation of practical advice based on interviews and comments from more than 60 chief information officers and IT leaders, and it includes many other proven ideas that if implemented will successfully reduce IT costs. 2009, 296 pages. **3-JR**

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**

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 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-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
WCM20000	Mapping of ISO/IEC 20000 with COBIT 4.1	25.00	Free
WCMCMM2	Mapping of CMMI for Development V1.2 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
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
1-IIA	A New Auditor's Guide to Planning, Performing, and Presenting IT Audits	80.00	70.00
5-ART	Outsourcing Information Security	103.00	93.00
7-SYN9	PCI Compliance, Second Edition	70.00	60.00
26-CRC	A Practical Guide to Security Assessments	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	100.00	90.00
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

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

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

19-M24	24 Deadly Sins of Software Security: Programming Flaws and How to Fix Them	60.00	50.00
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
11-EL	Cyber Attacks: Protecting National Infrastructure	70.00	60.00
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
23-MHE	Hacking Exposed Web Applications, 3rd 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

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

ISACA Bookstore Price List

Code	Title	Nonmember	Member
21-MMS	Mobile Application Security	60.00	50.00
86-WNS	Network Security Bible, 2nd Edition	70.00	60.00
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
24-MSIEM	Security Information and Event Management (SIEM) Implementation	75.00	65.00
1-OSM	Security Monitoring	55.00	45.00
2-JBSF	System Forensics, Investigation, and Response	93.00	83.00
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
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
89-WEG	Empowering Green Initiatives with IT: A Strategy and Implementation Guide	60.00	50.00
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
5-AS11	IT Governance: Policies & Procedures, 2011 Edition	235.00	225.00
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
25-MIPM	IT Project Management: On Track from Start to Finish, 3rd Edition	60.00	50.00
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
3-JR	A Practical Guide to Reducing IT Costs	60.00	50.00
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
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

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

FOUR EASY WAYS TO PLACE AN ORDER:

Online
Order online at
www.isaca.org/bookstore

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

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

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

RETURN POLICY

All purchases are final. No refunds or exchanges.

PUBLICATION QUANTITY DISCOUNTS

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

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

ISACA® Customer Order Form

Trust in, and value from, information systems

OFFICE USE ONLY

Vol. 3 -11

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

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

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

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.

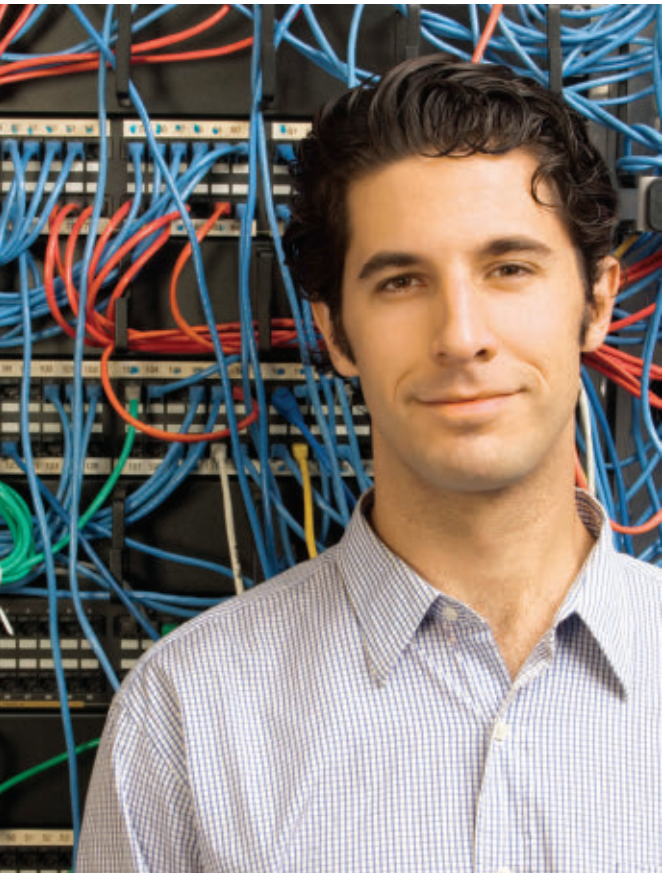
For Orders Totaling	Outside US	Within US
Up to US $30.00	US $10.00	US $5.00
US $30.01 to US $50.00	US $15.00	US $7.00
US $50.01 to US $80.00	US $20.00	US $8.00
US $80.01 to US $150.00	US $26.00	US $10.00
Over US $150.00	17% of Total	10% of Total

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.**

KEEP YOUR CAREER ON TRACK



At Regis University, we believe that information assurance professionals should have the knowledge to maximize the use of data within an organization as well as protect it. As a result, our Information Assurance programs are grounded in security but also focus on delivering the requisite combination of IT and business acumen — **creating a link between the server room and the boardroom.**

Available programs – online or on-campus:

MASTER OF SCIENCE IN INFORMATION ASSURANCE

- General track
- Specialization in Cyber Security
- Specialization in Information Assurance Policy Management

Regis University is designated as a Center of Academic Excellence in Information Assurance Education by the National Security Agency. The curriculum is modeled on the guidelines and recommendations provided by the Committee on National Security Systems (CNSS) 4000 training standards, the (ISC)² International Information Systems Security Certification Consortium Ten Domains of Knowledge, and ISACA.

The program can be taken on campus or completely online

REGIS UNIVERSITY
School of Computer & Information Sciences

LEARN MORE

RegisDegrees.com/ISACA | 1-877-820-0581